Probabilistic Timed Automata with Clock-Dependent Probabilities

Probabilistic Timed Automata with Clock-Dependent Probabilities

Jeremy Sproston
Dipartimento di Informatica, University of Turin, Italy
sproston@di.unito.it

Abstract

Probabilistic timed automata are classical timed automata extended with discrete probability distributions over edges. We introduce clock-dependent probabilistic timed automata, a variant of probabilistic timed automata in which transition probabilities can depend linearly on clock values. Clock-dependent probabilistic timed automata allow the modelling of a continuous relationship between time passage and the likelihood of system events. We show that the problem of deciding whether the maximum probability of reaching a certain location is above a threshold is undecidable for clock-dependent probabilistic timed automata. On the positive side, we show that the maximum and minimum probability of reaching a certain location in clock-dependent probabilistic timed automata can be approximated using a region-graph-based approach.

1 Introduction

Reactive systems are increasingly required to satisfy a combination of qualitative criteria (such as safety and liveness) and quantitative criteria (such as timeliness, reliability and performance). This trend has led to the development of techniques and tools for the formal verification of both qualitative and quantitative properties. In this paper, we consider a formalism for real-time systems that exhibit randomised behaviour, namely probabilistic timed automata (PTA) [1, 2]. PTA extend classical Alur-Dill timed automata [3] with discrete probabilistic branching over automata edges; alternatively a PTA can be viewed as a Markov decision process [4] or a Segala probabilistic automaton [5] extended with timed-automata-like clock variables and constraints over those clocks. PTA have been used previously to model case studies including randomised protocols and scheduling problems with uncertainty [6, 7], some of which have become standard benchmarks in the field of probabilistic model checking.

We recall briefly the behaviour of a PTA: as time passes, the model stays within a particular discrete state, and the values of its clocks increase at the same rate; at a certain point in time, the model can leave the discrete state if the current values of the clocks satisfy a constraint (called a guard) labelling one of the probability distributions over edges leaving the state; then a probabilistic choice as to which discrete state to then visit is made according to the chosen distribution over edges. In the standard presentation of PTA, any dependencies between time and probabilities over edges must be defined by utilising multiple distributions enabled with different sets of clock values. For example, to model the fact that a packet loss is more likely as time passes, we can use clock x to measure time, and two distributions μ_1 and μ_2 assigning probability λ_1 and λ_2 (for $\lambda_1 < \lambda_2$), respectively, to taking edges leading to a discrete state corresponding to packet loss, where the guard of μ_1 is $x \leq c$ and the guard of μ_2 is $x > c$, for some constant $c \in \mathbb{N}$. Hence, when the value of clock x is not more than c, a packet

loss occurs with probability λ_1, otherwise it occurs with probability λ_2. A more direct way of expressing the relationship between time and probability would be letting the probability of making a transition to a discrete state representing packet loss be dependent on the value of the clock, i.e., let the value of this probability be equal to $f(x)$, where f is an increasing function from the values of x to probabilities. We note that such a kind of dependence of discrete branching probabilities on values of continuous variables is standard in the field of stochastic hybrid systems, for example in [8].

In this paper we consider such a formalism based on PTA, in which all probabilities used by edge distributions can be expressed as functions of values of the clocks used by the model: the resulting formalism is called *clock-dependent probabilistic timed automata* (cdPTA). We focus on a simple class of functions from clock values to probabilities, namely those that can be expressed as sums of continuous linear functions, and consider a basic problem in the context of probabilistic model checking, namely probabilistic reachability: determine whether the maximum (respectively, minimum) probability of reaching a certain set of discrete states from the initial state is above (respectively, below) a threshold. After introducing cdPTA (in Section 2), our first result (in Section 3) is that the probabilistic reachability problem is undecidable for cdPTA with a least three clocks. This result is inspired from recent related work on stochastic timed Markov decision processes [9]. Furthermore, we give an example of cdPTA with one clock for which the maximal probability of reaching a certain discrete state involves a particular edge being taken when the clock has an irrational value. This suggests that classical techniques for partitioning the state space into a finite number of equivalence classes on the basis of a fixed, rational-numbered time granularity, such as the region graph [3] or the corner-point abstraction [10], cannot be applied directly to the case of cdPTA to obtain optimal reachability probabilities, because they rely on the fact that optimal choices can be made either at or arbitrarily closely to clock values that are multiples of the chosen rational-numbered time granularity. In Section 4, we present a conservative approximation method for cdPTA, i.e., maximum (respectively, minimum) probabilities are bounded from above (respectively, from below) in the approximation. This method is based on the region graph but uses concepts from the corner-point abstraction to define transition distributions. We show that successive refinement of the approximation, obtained by increasing the time granularity by a constant factor, does not lead to a more conservative approximation: in practice, in many cases such a refinement can lead to a substantial improvement in the computed probabilities, as we show using a small example. Furthermore, we show that, for the class of cdPTA for which the target states can only be reached within a bounded number of steps, for any time granularity, we can obtain a bound on the difference of the probabilities computed on the approximation and those of the cdPTA, and that increasing the time granularity results in a quantifiable improvement in the bound. This final result, together with proofs of all results and additional examples, extends the workshop version of the paper [11]. This paper is a post-print version of [12].

2 Clock-Dependent Probabilistic Timed Automata

2.1 Preliminaries

We use $\mathbb{R}_{\geq 0}$ to denote the set of non-negative real numbers, $\mathbb{Q}$ to denote the set of rational numbers and $\mathbb{N}$ to denote the set of natural numbers. A (discrete) probability *distribution* over a countable set Q is a function $\mu : Q \to [0,1]$ such that $\sum_{q \in Q} \mu(q) = 1$. For a function $\mu : Q \to \mathbb{R}_{\geq 0}$ we define $\mathsf{support}(\mu) = \{q \in Q : \mu(q) > 0\}$. For an uncountable set Q we define $\mathsf{Dist}(Q)$ to be the set of functions $\mu : Q \to [0,1]$, such that $\mathsf{support}(\mu)$ is a countable

set and μ restricted to $\mathsf{support}(\mu)$ is a (discrete) probability distribution. Given $q \in Q$, we use $\{q \mapsto 1\}$ to denote the distribution that assigns probability 1 to the single element q. Let $\{\mu_i\}_{i\in I} \subseteq \mathsf{Dist}(Q)$ be a set of distributions and $\{\lambda_i\}_{i\in I}$ be a set of weights such that $\lambda_i > 0$ for all $i \in I$ and $\sum_{i\in I} \lambda_i = 1$. Then we write $\bigoplus_{i\in I} \lambda_i \cdot \mu_i$ to refer to the distribution over Q such that $(\bigoplus_{i\in I} \lambda_i \cdot \mu_i)(q) = \sum_{i\in I} \lambda_i \cdot \mu_i(q)$ for each $q \in Q$.

A *probabilistic transition system* (PTS) $\mathcal{T} = (S, \overline{s}, Act, \Delta)$ comprises the following components: a set S of *states* with an *initial state* $\overline{s} \in S$, a set Act of *actions*, and a *probabilistic transition relation* $\Delta \subseteq S \times Act \times \mathsf{Dist}(S)$. The sets of states, actions and the probabilistic transition relation can be uncountable. Transitions from state to state of a PTS are performed in two steps: if the current state is s, the first step concerns a nondeterministic selection of a probabilistic transition $(s, a, \mu) \in \Delta$; the second step comprises a probabilistic choice, made according to the distribution μ, as to which state to make the transition (that is, a transition to a state $s' \in S$ is made with probability $\mu(s')$). We denote such a completed transition by $s \xrightarrow{a,\mu} s'$. We assume that for each state $s \in S$ there exists some $(s, a, \mu) \in \Delta$.

An *infinite run* of the PTS $\mathcal{T}$ is an infinite sequence of consecutive transitions $r = s_0 \xrightarrow{a_0,\mu_0} s_1 \xrightarrow{a_1,\mu_1} \cdots$ (i.e., the target state of one transition is the source state of the next). Similarly, a *finite run* of $\mathcal{T}$ is a finite sequence of consecutive transitions $r = s_0 \xrightarrow{a_0,\mu_0} s_1 \xrightarrow{a_1,\mu_1} \cdots \xrightarrow{a_{n-1},\mu_{n-1}} s_n$. We use $\mathit{InfRuns}^{\mathcal{T}}$ to denote the set of infinite runs of $\mathcal{T}$, and $\mathit{FinRuns}^{\mathcal{T}}$ the set of finite runs of $\mathcal{T}$. If r is a finite run, we denote by $\mathit{last}(r)$ the last state of r. For any infinite run r and $i \in \mathbb{N}$, let $r(i) = s_i$ be the $(i+1)$th state along r. Let $\mathit{FinRuns}^{\mathcal{T}}(s)$ and $\mathit{InfRuns}^{\mathcal{T}}(s)$ refer to the set of finite and infinite runs of $\mathcal{T}$, respectively, commencing in state $s \in S$.

A *strategy* of a PTS $\mathcal{T}$ is a function σ mapping every finite run $r \in \mathit{FinRuns}^{\mathcal{T}}$ to a distribution in $\mathsf{Dist}(\Delta)$ such that $(s, a, \mu) \in \mathsf{support}(\sigma(r))$ implies that $s = \mathit{last}(r)$. From [13, Lemma 4.10], without loss of generality we can assume henceforth that strategies map to distributions assigning positive probability to finite sets of elements, i.e., strategies σ for which $|\mathsf{support}(\sigma(r))|$ is finite for all $r \in \mathit{FinRuns}^{\mathcal{T}}$. Let $\Sigma^{\mathcal{T}}$ be the set of strategies of $\mathcal{T}$; when clear from the context, we write simply Σ. For any strategy σ, let $\mathit{FinRuns}^{\sigma}$ and $\mathit{InfRuns}^{\sigma}$ denote the set of finite and infinite runs, respectively, resulting from the choices of σ. For a state $s \in S$, let $\mathit{FinRuns}^{\sigma}(s) = \mathit{FinRuns}^{\sigma} \cap \mathit{FinRuns}^{\mathcal{T}}(s)$ and $\mathit{InfRuns}^{\sigma}(s) = \mathit{InfRuns}^{\sigma} \cap \mathit{InfRuns}^{\mathcal{T}}(s)$.

Given a strategy σ and a state $s \in S$, we define the probability measure $\Pr_s^{\sigma}$ over $\mathit{InfRuns}^{\sigma}(s)$ in the following, standard way [14]. A *Markov chain* (MC) $\mathcal{M} = (\mathbf{S}, \overline{\mathbf{s}}, \mathbf{P})$ comprises a set $\mathbf{S}$ of states with the initial state $\overline{\mathbf{s}} \in \mathbf{S}$, and a probabilistic transition function $\mathbf{P} : \mathbf{S} \times \mathbf{S} \to [0, 1]$, such that $\sum_{\mathbf{s}'\in\mathbf{S}} \mathbf{P}(\mathbf{s}, \mathbf{s}') = 1$ for all $\mathbf{s} \in \mathbf{S}$. Given a PTS $\mathcal{T} = (S, \overline{s}, Act, \Delta)$, a state $s \in S$, and a strategy $\sigma \in \Sigma$, we can define a countably infinite-state MC $\mathcal{M}_s^{\sigma} = (\mathit{FinRuns}^{\sigma}(s), s, \mathbf{P}_s^{\sigma})$, where $\mathbf{P}_s^{\sigma}$ is defined in the following way: for $r, r' \in \mathit{FinRuns}^{\sigma}(\overline{s})$, we let $\mathbf{P}_s^{\sigma}(r, r') = \sigma(r)(\mathit{last}(r), a, \mu) \cdot \mu(s')$ if $r' = r \xrightarrow{a,\mu} s'$, and we let $\mathbf{P}_s^{\sigma}(r, r') = 0$ otherwise. For a finite path $r \in \mathit{FinRuns}^{\sigma}(s)$, where $r = s_0 \xrightarrow{a_0,\mu_0} s_1 \xrightarrow{a_1,\mu_1} \cdots \xrightarrow{a_{n-1},\mu_{n-1}} s_n$, and $i \leq n$ let $r{\downarrow_i} = s_0 \xrightarrow{a_0,\mu_0} s_1 \xrightarrow{a_1,\mu_1} \cdots \xrightarrow{a_{i-1},\mu_{i-1}} s_i$. Then we let $\mathbf{P}_s^{\sigma}(r) = \mathbf{P}_s^{\sigma}(r{\downarrow_0}, r{\downarrow_1}) \cdot \mathbf{P}_s^{\sigma}(r{\downarrow_1}, r{\downarrow_2}) \cdot \ldots \cdot \mathbf{P}_s^{\sigma}(r{\downarrow_{n-1}}, r{\downarrow_n})$. Let $\mathsf{Cyl}(r) \subseteq \mathit{InfRuns}^{\sigma}(s)$ be the set of infinite runs with r as a prefix, and let $\Pr_s^{\sigma}$ be the unique measure such that $\Pr_s^{\sigma}(\mathsf{Cyl}(r)) = \mathbf{P}_s^{\sigma}(r)$.

Given a set $S_F \subseteq S$, define $\Diamond S_F = \{r \in \mathit{InfRuns}^{\mathcal{T}} : \exists i \in \mathbb{N} \text{ s.t. } r(i) \in S_F\}$ to be the set of infinite runs of $\mathcal{T}$ such that some state of S_F is visited along the run. Given a set $\Sigma' \subseteq \Sigma$ of strategies, we define the *maximum value over* Σ' *with respect to* S_F as $\mathbb{P}^{\max}_{\mathcal{T},\Sigma'}(S_F) = \sup_{\sigma\in\Sigma'} \Pr_{\overline{s}}^{\sigma}(\Diamond S_F)$. Similarly, the *minimum value over* Σ' *with respect to* S_F is defined as $\mathbb{P}^{\min}_{\mathcal{T},\Sigma'}(S_F) = \inf_{\sigma\in\Sigma'} \Pr_{\overline{s}}^{\sigma}(\Diamond S_F)$. The *maximal reachability problem* for $\mathcal{T}$, $S_F \subseteq S$, $\Sigma' \subseteq \Sigma$, $\trianglerighteq \in \{\geq, >\}$ and $\lambda \in [0, 1]$ is to decide whether $\mathbb{P}^{\max}_{\mathcal{T},\Sigma'}(S_F) \trianglerighteq \lambda$. Similarly, the *minimal reachability problem* for $\mathcal{T}$, $S_F \subseteq S$, $\Sigma' \subseteq \Sigma$, $\trianglelefteq \in \{\leq, <\}$ and $\lambda \in [0, 1]$ is to decide whether $\mathbb{P}^{\min}_{\mathcal{T},\Sigma'}(S_F) \trianglelefteq \lambda$.

Let $\equiv \subseteq S \times S$ be an equivalence relation over S. We say that $\equiv$ *respects* $S' \subseteq S$ if S' is

the union of states contained in some set of equivalence classes of $\equiv$. Given two distributions μ, μ' over S, we write $\mu \equiv \mu'$ if $\sum_{s \in C} \mu(s) = \sum_{s \in C} \mu'(s)$ for all equivalence classes C of $\equiv$. A *combined transition* from state $s \in S$ is a pair $(\{(s, a_i, \mu_i)\}_{i \in I}, \{\lambda_i\}_{i \in I})$ such that $(s, a_i, \mu_i) \in \Delta$ and $\lambda_i > 0$ for all $i \in I$, and $\sum_{i \in I} \lambda_i = 1$. Let $A \subseteq Act$ be a set of actions. Then a *probabilistic simulation respecting* $\equiv$ *and* A is a relation $\preceq \subseteq S \times S$ such that $s \preceq t$ implies that (1) $s \equiv t$, and (2) for each transition $(s, a, \mu) \in \Delta$, there exists a combined transition $(\{(t, a_i, \mu_i)\}_{i \in I}, \{\lambda_i\}_{i \in I})$ such that $\mu \equiv \bigoplus_{i \in I} \lambda_i \cdot \mu_i$, $\{a_i\}_{i \in I} \subseteq A$ if $a \in A$, and $\{a_i\}_{i \in I} \subseteq Act \setminus A$ if $a \in Act \setminus A$.[1]

Next, we consider strategies that alternate between actions in a certain set $A \subseteq Act$ and actions in the complement set $Act \setminus A$. Formally, an *A-alternating strategy* σ is a strategy such that, for finite run $r \in FinRuns^{\mathcal{T}}$ that has $s \xrightarrow{a,\mu} s'$ as its final transition, then $\{a' \in Act : (s, a', \mu) \in \mathsf{support}(\sigma(r))\} \subseteq A$ if $a \in Act \setminus A$, and $\{a' \in Act : (s, a', \mu) \in \mathsf{support}(\sigma(r))\} \subseteq Act \setminus A$ if $a \in A$. Let $\Sigma_A^{\mathcal{T}}$ be the set of A-alternating strategies of $\mathcal{T}$; when the context is clear, we write simply Σ_A rather than $\Sigma_A^{\mathcal{T}}$.

Given two PTSs $\mathcal{T}_1 = (S_1, \overline{s}_1, Act_1, \Delta_1)$ and $\mathcal{T}_2 = (S_2, \overline{s}_2, Act_2, \Delta_2)$, their disjoint union is defined as the PTS $(S_1 \uplus S_2, \_, Act_1 \uplus Act_2, \Delta_1 \uplus \Delta_2)$ (where the initial state is irrelevant and is hence omitted). The following result is essentially identical to [13, Lemma 3.17, Lemma 3.18] (which in turn relies on [5, Theorem 8.6.1]).

Proposition 1. *[13] Let $A_1 \subseteq Act_1$, let $A_2 \subseteq Act_2$, and let $\equiv$ be an equivalence relation over $S_1 \uplus S_2$ that respects S_F . If $\overline{s}_1 \preceq \overline{s}_2$ for a probabilistic simulation respecting $\equiv$ and $A_1 \uplus A_2$, then $\mathbb{P}^{\max}_{\mathcal{T}_1, \Sigma_{A_1}}(S_F) \leq \mathbb{P}^{\max}_{\mathcal{T}_2, \Sigma_{A_2}}(S_F)$ and $\mathbb{P}^{\min}_{\mathcal{T}_1, \Sigma_{A_1}}(S_F) \geq \mathbb{P}^{\min}_{\mathcal{T}_2, \Sigma_{A_2}}(S_F)$.*

2.2 Clock-Dependent Probabilistic Timed Automata

Let $\mathcal{X}$ be a finite set of real-valued variables called *clocks*, the values of which increase at the same rate as real-time and which can be reset to 0. A function $v : \mathcal{X} \to \mathbb{R}_{\geq 0}$ is referred to as a *clock valuation* and the set of all clock valuations is denoted by $\mathbb{R}^{\mathcal{X}}_{\geq 0}$. For $v \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$, $t \in \mathbb{R}_{\geq 0}$ and $X \subseteq \mathcal{X}$, we use $v{+}t$ to denote the clock valuation that increments all clock values in v by t, and $v[X{:=}0]$ to denote the clock valuation in which clocks in X are reset to 0. Formally, $(v{+}t)(x) = v(x){+}t$ for all $x \in \mathcal{X}$, $v[X{:=}0](x) = 0$ for all $x \in X$, and $v[X{:=}0](x) = v(x)$ for all $x \in \mathcal{X} \setminus X$.

For a set Q, a *distribution template* $\mathfrak{d} : \mathbb{R}^{\mathcal{X}}_{\geq 0} \to \mathsf{Dist}(Q)$ gives a distribution over Q for each clock valuation. In the following, we use notation $\mathfrak{d}[v]$, rather than $\mathfrak{d}(v)$, to denote the distribution corresponding to distribution template $\mathfrak{d}$ and clock valuation v. Let $\mathfrak{Templates}(Q)$ be the set of distribution templates over Q.

The set $CC(\mathcal{X})$ of *clock constraints* over $\mathcal{X}$ is defined as the set of conjunctions over atomic formulae of the form $x \sim c$, where $x \in \mathcal{X}$, $\sim \in \{<, \leq, \geq, >\}$ and $c \in \mathbb{N}$. A clock valuation v satisfies a clock constraint ψ, denoted by $v \models \psi$, if ψ resolves to `true` when substituting each occurrence of clock x with $v(x)$.

A *clock-dependent probabilistic timed automaton* (cdPTA) $\mathcal{P} = (L, \bar{l}, \mathcal{X}, inv, prob)$ comprises the following components:

- a finite set L of *locations* with an *initial location* $\bar{l} \in L$;
- a finite set $\mathcal{X}$ of clocks;

[1] Our notion of probabilistic simulation respecting an equivalence relation is stronger than that of probabilistic simulation of [5], because in our setting we require that the distributions referred to in the definition assign the *same* probability to equivalence classes, whereas the standard definition of probabilistic simulation requires that corresponding transitions should be related by a weight function based on the probabilistic simulation preorder. Also note that we do not require actions to be matched in the definition of probabilistic simulation respecting $\equiv$, although we *do* require that matching actions are either all in A or all in $Act \setminus A$: in this paper, we use actions in later sections only to clarify aspects of correctness proofs.

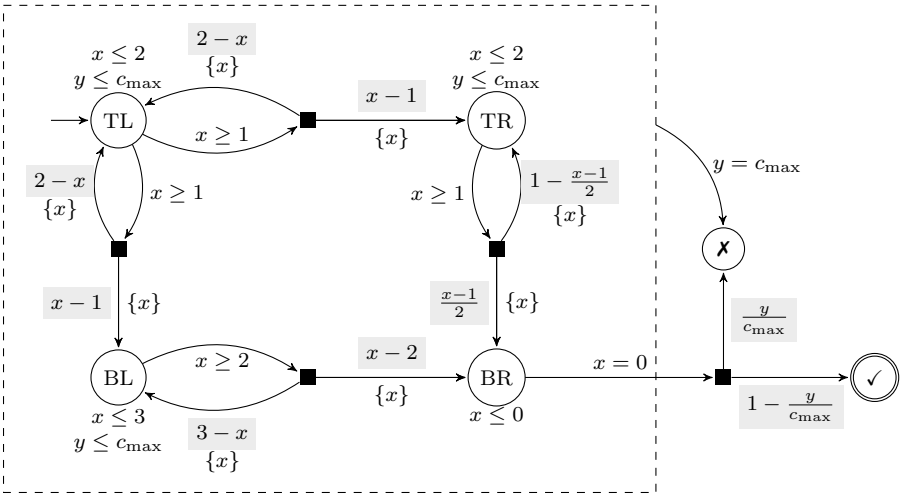

Figure 1: A cdPTA modelling a simple robot example.

- a function $inv : L \to CC(\mathcal{X})$ associating an *invariant condition* with each location;
- a set $prob \subseteq L \times CC(\mathcal{X}) \times \mathfrak{Templates}(2^{\mathcal{X}} \times L)$ of *probabilistic edges*.

A probabilistic edge $(l, g, \mathfrak{p}) \in prob$ comprises: (1) a source location l; (2) a clock constraint g, called a *guard*; and (3) a distribution template $\mathfrak{p}$ with respect to pairs of the form $(X, l') \in 2^{\mathcal{X}} \times L$ (i.e., pairs consisting of a set X of clocks to be reset and a target location l').

The behaviour of a cdPTA takes a similar form to that of a standard probabilistic timed automaton [1, 2]: in any location time can advance as long as the invariant holds, and the choice as to how much time elapses is made nondeterministically; a probabilistic edge can be taken if its guard is satisfied by the current values of the clocks, and the choice as to which probabilistic edge to take is made nondeterministically; for a taken probabilistic edge, the choice of which clocks to reset and which target location to make the transition to is *probabilistic*. The key difference with cdPTA is that the distribution used to make this probabilistic choice depends on the probabilistic edge taken *and* on the current clock valuation.

Example 1. *In Figure 1 we give an example of a cdPTA modelling a simple robot that must reach a certain geographical area and then carry out a particular task. The usual conventions for the graphical representation of timed automata are used in the figure. Black squares denote the distributions of probabilistic edges, and expressions on probabilities used by distribution templates are written with a grey background labelling their outgoing arcs. Edges without black squares correspond to probabilistic edges assigning probability* 1 *to a single clock set/target location pair. The robot can be in one of four geographical areas, which can be thought of as cells in a* 2×2 *grid, each of which corresponds to a cdPTA location. The robot begins in the top-left cell (corresponding to location* TL*), and its objective is to reach the bottom-right cell (location* BR*). From the top-left cell, the robot can move either to the top-right cell (location* TR*), or to the bottom-left cell (location* BL*). In each cell, the robot must wait a certain amount of time (*1 *time units in the top cells and* 2 *time units in the bottom-left cell) before attempting to leave the cell (for example, to recharge solar batteries), after which it can spend at most* 1 *time unit attempting to leave the cell. With a certain probability, the attempt to leave the cell will fail. The more time dedicated to an attempt to leave the cell, the more likely the attempt will succeed. If the attempt to leave the cell fails, the robot must wait before trying to leave the cell again. Although passing through the top-right cell is not slower than passing through the bottom-left cell, the probability of leaving the cell successfully increases at a slower rate than in other cells (hence, the top-right cell could represent a short route to the bottom-right cell, but*

through terrain in which the robot finds it difficult to navigate). On arrival in the bottom-right cell, the robot successfully carries out its task with a probability that is inversely proportional to the total time elapsed (for example, the robot could be transporting medical supplies, the efficacy of which may be inversely proportional to the time elapsed). The clock x is used to represent the amount of time used by the robot in its attempt to move from cell to cell, whereas the clock y represents the total amount of time since the start of the robot's mission. If the clock y reaches its maximum amount $c_{\max}$, then the mission fails (as denoted by the edge to the location denoted by ✗, which is available in locations TL, TR, BL *and* BR*, as indicated by the dashed box). The objective of the robot's controller is to maximise the probability of reaching the location denoted by ✓. Note that there is a trade-off between dedicating more time to movement between the cells, which increases the probability of successful navigation and therefore progress towards the target point, and spending less time on the overall mission, which increases the probability of carrying out the required task at the target point.*

A *state* of a cdPTA is a pair comprising a location and a clock valuation satisfying the location's invariant condition, i.e., $(l, v) \in L \times \mathbb{R}^{\mathcal{X}}_{\geq 0}$ such that $v \models \mathit{inv}(l)$. In any state (l, v), either a certain amount of time $\delta \in \mathbb{R}_{\geq 0}$ elapses, or a probabilistic edge is traversed. If time elapses, then the choice of δ requires that the invariant $\mathit{inv}(l)$ remains continuously satisfied while time passes. The resulting state after this transition is $(l, v{+}\delta)$. A probabilistic edge $(l', g, \mathfrak{p}) \in \mathit{prob}$ can be chosen from state (l, v) if $l = l'$ and it is *enabled*, i.e., the clock constraint g is satisfied by v. Once a probabilistic edge $(l, g, \mathfrak{p})$ is chosen, a set of clocks to reset to 0 and a successor location are selected at random, according to the distribution $\mathfrak{p}[v]$. Note that the fundamental difference between cdPTA and the standard PTA formalism concerns the fact that, in PTA, the third component of edges is a distribution, rather than a distribution template, and hence the probabilities used in a PTA do not depend on valuations.

We make a number of assumptions concerning the cdPTA models considered. These assumptions are standard for PTA, and enable the definition of (cd)PTA semantics. Firstly, we restrict our attention to cdPTA for which it is always possible to take a probabilistic edge, either immediately or after letting time elapse. This condition holds generally for PTA models in practice [6]. A sufficient syntactic condition for this property has been presented formally in [15]. Secondly, in the standard manner for PTA [7], we assume that all possible target states of probabilistic edges satisfy their invariants: for all probabilistic edges $(l, g, \mathfrak{p}) \in \mathit{prob}$, for all clock valuations $v \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$ such that $v \models g$, and for all $(X, l') \in 2^{\mathcal{X}} \times L$, we have that $\mathfrak{p}[v](X, l') > 0$ implies $v[X := 0] \models \mathit{inv}(l')$. Thirdly, we assume that any clock valuation that satisfies the guard of a probabilistic edge also satisfies the invariant of the source location: this can be achieved, without changing the underlying semantic PTS, by replacing each probabilistic edge $(l, g, \mathfrak{p}) \in \mathit{prob}$ by $(l, g \wedge \mathit{inv}(l), \mathfrak{p})$. Finally, we consider cdPTA that feature invariant conditions that prevent clock values from exceeding some bound: formally, for each location $l \in L$, we have that $\mathit{inv}(l)$ contains a constraint of the form $x \leq c$ or $x < c$ for each clock $x \in \mathcal{X}$ (this assumption is not necessary for the definition of the semantics of cdPTA, but will simplify the material in subsequent sections).[2]

Let $\mathbf{0} \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$ be the clock valuation that assigns 0 to all clocks in $\mathcal{X}$. The semantics of the cdPTA $\mathcal{P} = (L, \bar{l}, \mathcal{X}, \mathit{inv}, \mathit{prob})$ is the PTS $[\![\mathcal{P}]\!] = (S, \bar{s}, \mathit{Act}, \Delta)$ where:

- $S = \{(l, v) : l \in L \text{ and } v \in \mathbb{R}^{\mathcal{X}}_{\geq 0} \text{ s.t. } v \models \mathit{inv}(l)\}$ and $\bar{s} = \{(\bar{l}, \mathbf{0})\}$;
- $\mathit{Act} = \mathbb{R}_{\geq 0} \cup \mathit{prob}$;

[2] Note that we relax some of these assumptions when depicting cdPTA graphically. For example, we generally depict final locations, and sink locations that cannot reach a target location, without invariant conditions or outgoing edges. To satisfy the above assumptions, we can equip each such a location with an invariant condition $x \leq M$ for some clock x, where M is the greatest constant featured in guards or invariant conditions of the cdPTA, and with a self-loop probabilistic edge with guard $x \leq M$ and a clock reset set $\{x\}$.

- $\Delta = \overrightarrow{\Delta} \cup \widehat{\Delta}$, where $\overrightarrow{\Delta} \subseteq S \times \mathbb{R}_{\geq 0} \times \mathsf{Dist}(S)$ and $\widehat{\Delta} \subseteq S \times \mathit{prob} \times \mathsf{Dist}(S)$ such that:
  - $\overrightarrow{\Delta}$ is the smallest set such that $((l,v),\delta,\{(l,v+\delta) \mapsto 1\}) \in \overrightarrow{\Delta}$ if there exists $\delta \in \mathbb{R}_{\geq 0}$ such that $v + \delta' \models \mathit{inv}(l)$ for all $0 \leq \delta' \leq \delta$;
  - $\widehat{\Delta}$ is the smallest set such that $((l,v),(l,g,\mathfrak{p}),\mu) \in \widehat{\Delta}$ if
    1. $v \models g$;
    2. for any $(l',v') \in S$, we have $\mu(l',v') = \sum_{X \in \mathsf{Reset}(v,v')} \mathfrak{p}[v](X,l')$, where $\mathsf{Reset}(v,v') = \{X \subseteq \mathcal{X} \mid v[X := 0] = v'\}$.

When considering maximum and minimum values for cdPTA, we henceforth consider strategies that alternate between transitions from $\overrightarrow{\Delta}$ (time elapse transitions) and transitions from $\widehat{\Delta}$ (probabilistic edge transitions). Formally, a *cdPTA strategy* σ is a strategy such that, for a finite run $r \in \mathit{FinRuns}^{[\![\mathcal{P}]\!]}$ that has $s \xrightarrow{a,\mu} s'$ as its final transition, either $(s,a,\mu) \in \overrightarrow{\Delta}$ and $\mathsf{support}(\sigma(r)) \subseteq \widehat{\Delta}$, or $(s,a,\mu) \in \widehat{\Delta}$ and $\mathsf{support}(\sigma(r)) \subseteq \overrightarrow{\Delta}$. We write $\mathbf{\Sigma}$ for the set of cdPTA strategies of $[\![\mathcal{P}]\!]$. Given a set $F \subseteq L$ of locations, subsequently called *target locations*, we let $S_F = \{(l,v) \in S : l \in F\}$. Let $\trianglerighteq \in \{\geq, >\}$, $\trianglelefteq \in \{\leq, <\}$ and $\lambda \in [0,1]$: then the maximal (respectively, minimal) reachability problem for cdPTA is to decide whether $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!],\mathbf{\Sigma}}(S_F) \trianglerighteq \lambda$ (respectively, $\mathbb{P}^{\min}_{[\![\mathcal{P}]\!],\mathbf{\Sigma}}(S_F) \trianglelefteq \lambda$).

2.3 Linear Clock Dependencies

In this paper, we concentrate on a particular subclass of distribution templates based on linear functions. Let $x \in \mathcal{X}$ be a clock and $\psi \in CC(\mathcal{X})$ be a clock constraint. Let I_x^ψ be the interval containing the values of x of clock valuations that satisfy ψ: formally $I_x^\psi = \{v(x) \in \mathbb{R}_{\geq 0} : v \in \mathbb{R}^{\mathcal{X}}_{\geq 0} \text{ s.t. } v \models \psi\}$. Let $\overline{I_x^\psi}$ be the closure of I_x^ψ. For example, for $\psi = (x \geq 3) \wedge (x < 5) \wedge (y \leq 8)$, we have $I_x^\psi = [3,5)$, $\overline{I_x^\psi} = [3,5]$ and $I_y^\psi = \overline{I_y^\psi} = [0,8]$. We equip each probabilistic edge $p = (l,g,\mathfrak{p}) \in \mathit{prob}$, clock set/location pair $e = (X,l') \in 2^{\mathcal{X}} \times L$ and clock $x \in \mathcal{X}$, with a pair $(c_x^{p,e}, d_x^{p,e}) \in \mathbb{Q}^2$ of rational constants. We then define the linear function $f_x^{p,e}$ with domain $\overline{I_x^g}$ by $f_x^{p,e}(\gamma) = c_x^{p,e} + d_x^{p,e} \cdot \gamma$ for all $\gamma \in \overline{I_x^g}$. We make the following assumptions for each probabilistic edge $p \in \mathit{prob}$:

1. $\sum_{x \in \mathcal{X}} f_x^{p,e}(v(x)) \in [0,1]$ for each $e \in 2^{\mathcal{X}} \times L$ and $v \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$ such that $v \models g$;
2. $\sum_{e \in 2^{\mathcal{X}} \times L} \sum_{x \in \mathcal{X}} f_x^{p,e}(v(x)) = 1$ for each $v \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$ such that $v \models g$.

Then we say that the probabilistic edge p is *linear* if, for each $e \in 2^{\mathcal{X}} \times L$ and each $v \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$ such that $v \models g$, we have $\mathfrak{p}[v](e) = \sum_{x \in \mathcal{X}} f_x^{p,e}(v(x))$. We assume henceforth that all probabilistic edges of cdPTA are linear.[3]

Example 2. *Standard methods for the analysis of timed automata typically consist of a finite-state system that represents faithfully the original model. In particular, the region graph [3]*

[3] The original version of the paper [11] featured *piecewise* linear clock dependencies, where the functions defining clock dependencies are linear over intervals of clock values that are bounded by rationals. The version of clock dependencies presented in this paper is no less expressive, because such piecewise linear clock dependencies can be modelled by (1) scaling up all constants in guards, invariants and the endpoints of intervals used to define over which clock dependencies are linear so that the intervals used for defining clock dependencies have natural numbered endpoints, and (2) modelling a probabilistic edge with piecewise linear clock dependencies by *multiple* probabilistic edges with linear clock dependencies, where the guards of the new probabilistic edges encode the (scaled-up) intervals over which the original piecewise linear clock dependency functions were linear.

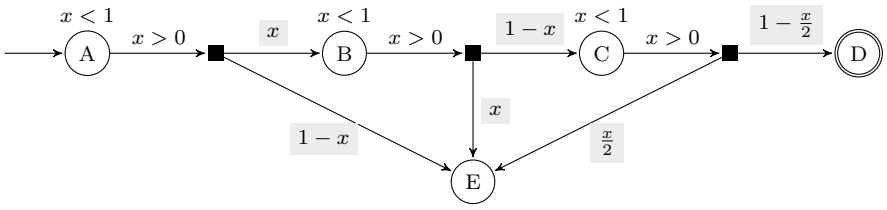

Figure 2: A one-clock cdPTA for which the maximum probability is attained by a time delay corresponding to an irrational number.

and the corner-point abstraction [10] both involve the division of the state space according to a fixed, rational-numbered granularity. The example of a one-clock cdPTA $\mathcal{P}$ of Figure 2 shows that such an approach cannot be used for the exact computation of optimal reachability probabilities in cdPTA, because optimality may be attained when the clock has an irrational value. For an example of the formal description of a linear probabilistic edge, consider the probabilistic edge from location C*, which we denote by p_{C}: then we have $I_x^{p_{\mathrm{C}}} = (0, 1)$, with $c_x^{p_{\mathrm{C}},(\emptyset,\mathrm{D})} = 1$, $d_x^{p_{\mathrm{C}},(\emptyset,\mathrm{D})} = -\frac{1}{2}$, $c_x^{p_{\mathrm{C}},(\emptyset,\mathrm{E})} = 0$, and $d_x^{p_{\mathrm{C}},(\emptyset,\mathrm{E})} = \frac{1}{2}$. Now consider the maximum probability of reaching location* D *(that is, $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!],\mathbf{\Sigma}}(S_{\{\mathrm{D}\}})$). Intuitively, the longer the cdPTA remains in location* A*, the lower the probability of making a transition to location* E *from* A*, but the higher the probability of making a transition to* E *from* B *and* C*. Note that, after* A *is left, the choice resulting in the maximum probability of reaching* D *is to take the outgoing transitions from* B *and* C *as soon as possible (delaying in* B *and* C *will increase the value of x, therefore increasing the probability of making a transition to* E*). Denoting by δ the amount of time elapsed in* A*, the maximum probability of reaching* D *is equal to $\delta(1-\delta)(1-\frac{\delta}{2})$, which (within the interval $[0, 1)$) reaches its maximum at $1 - \frac{\sqrt{3}}{3}$. Hence, this example indicates that abstractions based on the optimality of choices made at (or arbitrarily close to) rational-numbered clock values (such as the region graph or corner-point abstraction) do not yield exact analysis methods for cdPTA.*

3 Undecidability of Maximal Reachability for cdPTA

Theorem 1. *The maximal reachability problem is undecidable for cdPTA with at least 3 clocks.*

Proof. We proceed by reducing the non-halting problem for two-counter machines to the maximal reachability problem for cdPTA. The reduction has close similarities to a reduction presented in [9].

A two-counter machine $\mathcal{M} = (\mathcal{L}, \mathcal{C})$ comprises a set $\mathcal{L} = \{\ell_1, ..., \ell_n\}$ of instructions and a set $\mathcal{C} = \{\mathsf{c}_1, \mathsf{c}_2\}$ of counters. The instructions are of the following form (for $i, j, k \in \{1, ..., n\}$ and $m \in \{1, 2\}$):

1. $\ell_i : \mathsf{c}_m := \mathsf{c}_m + 1$; goto ℓ_j (increment c_m);
2. $\ell_i : \mathsf{c}_m := \mathsf{c}_m - 1$; goto ℓ_j (decrement c_m);
3. $\ell_i :$ if $(\mathsf{c}_m > 0)$ then goto ℓ_j else goto ℓ_k (zero check c_m);
4. ℓ_n : HALT (halting instruction).

A configuration $(\ell, \mathsf{v}_1, \mathsf{v}_2)$ of a two-counter machine comprises an instruction ℓ and values v_1 and v_2 of counters c_1 and c_2, respectively. The instruction of a configuration describes ow the counter values are to be updated and what is the next instruction to be executed (for example, an instruction $\ell_8 : \mathsf{c}_2 := \mathsf{c}_2 + 1$; goto ℓ_3 taken from configuration $(\ell_8, 6, 4)$

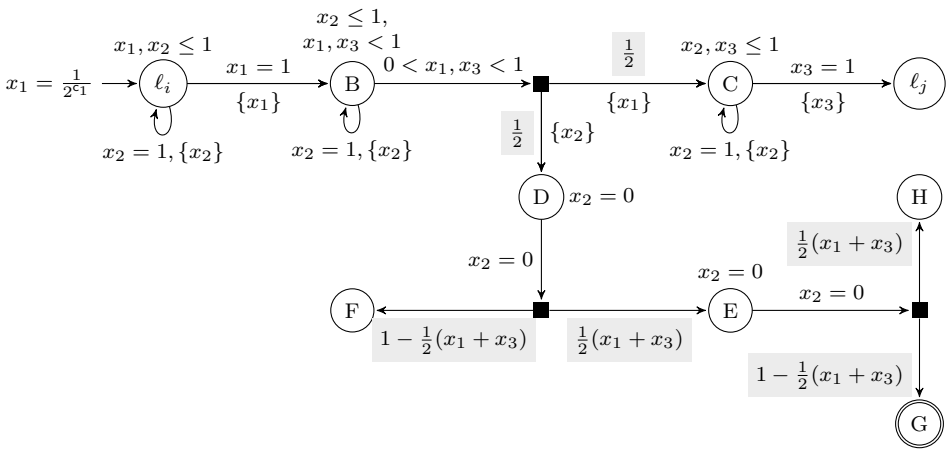

Figure 3: The cdPTA module for simulating an increment instruction for counter c_1.

results in the configuration $(\ell_3, 6, 5)$). A run of a two-counter machine consists of a finite or infinite sequence of configurations, starting from configuration $(\ell_1, 0, 0)$, and where subsequent configurations are successively generated by following the instruction specified in the associated configuration. A run is finite if and only if the final instruction visited along the run is ℓ_n (the halting instruction). The halting problem for two-counter machines concerns determining whether the unique run of the two-counter machine is finite, and is undecidable [16]; hence the non-halting problem (determining whether the unique run of the two-counter machine is infinite) is also undecidable.

Consider a two-counter machine $\mathcal{M}$. We reduce the non-halting problem for $\mathcal{M}$ to the maximal reachability problem of a cdPTA in the following way. We construct a cdPTA $\mathcal{P}_{\mathcal{M}}$ with three clocks $\{x_1, x_2, x_3\}$ by considering modules for each form that the instructions of a two-counter machine can take. On entry to each module, we have that $x_1 = \frac{1}{2^{c_1}}$, $x_2 = \frac{1}{2^{c_2}}$ and $x_3 = 0$. The module for simulating an increment instruction for c_1 is shown in Figure 3. In location ℓ_i, there is a delay of $1 - \frac{1}{2^{c_1}}$, and hence the values of the clocks on entry to location B are $x_1 = 0$, $x_2 = \frac{1}{2^{c_2}} + 1 - \frac{1}{2^{c_1}} \mod 1$ and $x_3 = 1 - \frac{1}{2^{c_1}}$. A nondeterministic choice is then made concerning the amount of time that elapses in location B: note that this amount must be in the interval $(0, \frac{1}{2^{c_1}})$. In order to correctly simulate the increment of counter c_1, the choice of delay in location B should be equal to $\frac{1}{2^{c_1+1}}$. On leaving location B, a probabilistic choice is made: the rightward outcome corresponds to continuing the simulation of the two-counter machine, whereas the downward outcome corresponds to checking that the delay in location B was correctly $\frac{1}{2^{c_1+1}}$. We write the delay in location B as $\frac{1}{2^{c_1+1}} + \epsilon$, where $-\frac{1}{2^{c_1+1}} < \epsilon < \frac{1}{2^{c_1+1}}$: hence, for a correct simulation of the increment of c_1, we require that $\epsilon = 0$.

Consider the case in which the downward outcome (from the outgoing probabilistic edge of location B) is taken: then the cdPTA fragment from location D has the role of checking whether $\epsilon = 0$. Note that, after entering location D, no time elapses in locations D and E (as enforced by the reset of x_2 to zero and the invariant condition $x_2 = 0$), and hence both clocks x_1 and x_3 retain the same values as they had when location B was left. We show that the probability of reaching the target location G from location D is $\frac{1}{4} - \epsilon^2$, and hence equal to $\frac{1}{4}$ if and only if $\epsilon = 0$. To see that the probability of reaching G from D is $\frac{1}{4} - \epsilon^2$, observe that the probability is equal to $\frac{1}{2}(x_1 + x_3) = \frac{1}{2}(\frac{1}{2^{c_1+1}} + \epsilon + (1 - \frac{1}{2^{c_1+1}}) + \epsilon) = \frac{1}{2} + \epsilon$ multiplied by $1 - \frac{1}{2}(x_1 + x_3) = \frac{1}{2} - \epsilon$, i.e., equal to $\frac{1}{4} - \epsilon^2$. Hence the probability of reaching location G from location D is equal to $\frac{1}{4}$ if and only if $\epsilon = 0$ (otherwise, the probability is strictly less than $\frac{1}{4}$).

The module for simulating a decrement instruction for counter c_1 is shown in Figure 4. In a similar manner to the cdPTA fragment in Figure 3 for the simulation of an increment instruction, the only nondeterministic choice made is with regard to the amount of time spent

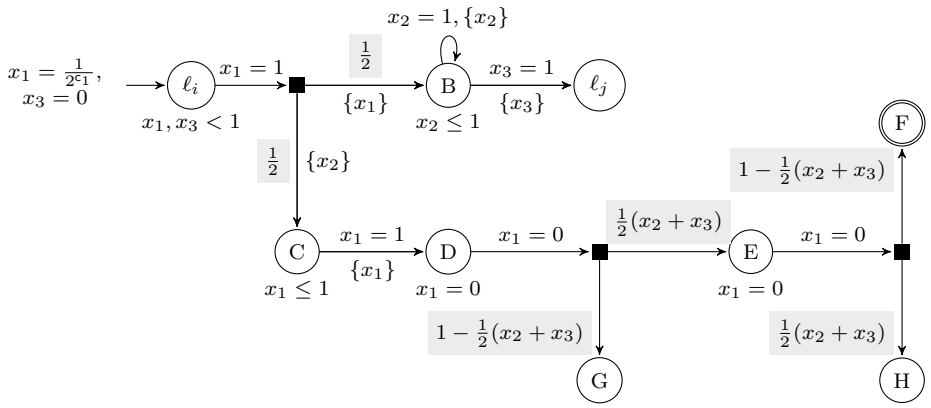

Figure 4: The cdPTA module for simulating a decrement instruction for counter c_1.

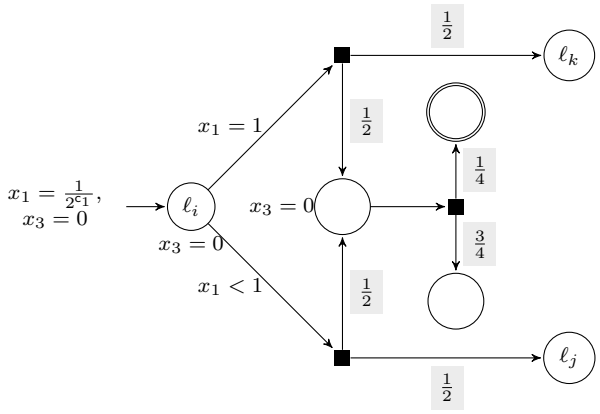

Figure 5: The cdPTA module for simulating a zero-test instruction for counter c_1.

in a location, in this case location ℓ_i. This amount of time is denoted by δ. For the correct simulation of the decrement instruction, δ should equal $1 - \frac{1}{2^{c_1 - 1}}$. The rightward outcome is taken from the probabilistic edge leaving location ℓ_i corresponds to the continuation of the simulation of the two-counter machine: hence, on entry to location B, we have $x_1 = 0$, $x_2 = \frac{1}{2^{c_2}} + \delta$ and $x_3 = \delta$; then, on entry to location ℓ_j, we have $x_1 = 1 - \delta$, $x_2 = \frac{1}{2^{c_2}}$ and $x_3 = 0$.

Let $\delta = 1 - \frac{1}{2^{c_1 - 1}} + \epsilon$. For the correct simulation of the decrement instruction, we require that $\epsilon = 0$. The downward outcome from the probabilistic edge leaving location ℓ_i corresponds to checking that $\epsilon = 0$, and takes a similar form to the analogous downward edge of the cdPTA fragment for the increment instruction, as shown in Figure 3. Note that, on entry to location C, we have that $x_1 = 1 - \frac{1}{2^{c_1}} + \epsilon$, $x_2 = 0$ and $x_3 = 1 - \frac{1}{2^{c_1 - 1}} + \epsilon$. Then, on entry to location D, we have that $x_1 = 0$, $x_2 = \frac{1}{2^{c_1}} - \epsilon$ and $x_3 = 1 - \frac{1}{2^{c_1}}$. As no time elapses in locations D and E, we have that target location F is then reached with probability $\frac{1}{2}(x_2 + x_3) = \frac{1}{2}(\frac{1}{2^{c_1}} - \epsilon + 1 - \frac{1}{2^{c_1}}) = \frac{1}{2} + \frac{\epsilon}{2}$ multiplied by the probability $1 - \frac{1}{2}(x_2 + x_3) = \frac{1}{2} - \frac{\epsilon}{2}$, which equals $\frac{1}{4} - \frac{\epsilon^2}{4}$. Hence we conclude that the probability of reaching location F from location C is equal to $\frac{1}{4}$ if $\epsilon = 0$, and is strictly less than $\frac{1}{4}$ otherwise.

Finally, the module for a zero test instruction ℓ_i : if $(\mathsf{c}_1 > 0)$ then goto ℓ_j else goto ℓ_k is shown in Figure 5. After entry to location ℓ_i, two probabilistic edges are enabled: the upper one is taken if $\mathsf{c}_1 = 0$ (i.e., if $x_1 = \frac{1}{2^0} = 1$), whereas the lower one is taken otherwise. Both probabilistic edges involve an outcome leading to location ℓ_j or ℓ_k (depending on which probabilistic edge was taken) with probability $\frac{1}{2}$, leading to a target location with probability $\frac{1}{2} \cdot \frac{1}{4}$, and leading to a sink, non-target location with probability $\frac{1}{2} \cdot \frac{3}{4}$, in exactly the same manner as the modules for increment and decrement.

Given the construction of a cdPTA simulating the two-counter machine using the modules described above, we can now proceed to show Theorem 1. The reasoning is the same as that of Lemma 5 of [9]. First note that, in the module of the cdPTA for simulating an instruction of the two-counter machine, if the strategy of the cdPTA simulates correctly a single step of the two-counter machine, then a target location is reached with probability $\frac{1}{2} \cdot \frac{1}{4}$ (i.e., probability $\frac{1}{2}$ for deciding to check the amount of time elapsed in a particular location multiplied by probability $\frac{1}{4}$ for the probability of reaching a target location when checking the amount of time elapsed, in both the increment and decrement modules, and probability $\frac{1}{2} \cdot \frac{1}{4}$ in the zero-test module, regardless of the value of the tested counter). If the two-counter machine halts in k steps, and the strategy of the cdPTA correctly simulates the two-counter machine the probability of reaching a target location will be $\frac{1}{2} \cdot \frac{1}{4} + (\frac{1}{2})^2 \cdot \frac{1}{4} + ... + (\frac{1}{2})^k \cdot \frac{1}{4} < \frac{1}{4}$. If the two-counter machine halts in k steps, and the strategy of the cdPTA does not correctly simulate the two-counter machine, then this means that the probability of reaching a target location is strictly less than that corresponding to correct simulation, given that deviation from simulation of a certain step corresponds to reaching the target locations with probability strictly less than $\frac{1}{4}$ in that step; hence the overall probability of reaching a target location will be strictly less than . $\frac{1}{2} \cdot \frac{1}{4} + (\frac{1}{2})^2 \cdot \frac{1}{4} + ... + (\frac{1}{2})^k \cdot \frac{1}{4} < \frac{1}{4}$. Now consider the case in which the two-counter machine does not halt: in this case, faithful simulation in the cdPTA corresponds to reaching target locations with probability $\sum_{i=1}^{\infty} (\frac{1}{2})^i \cdot \frac{1}{4} = \frac{1}{4}$, whereas unfaithful simulation in the cdPTA corresponds to reaching the target locations with probability $\sum_{i=1}^{\infty} (\frac{1}{2})^i \cdot \gamma_i$ where $\gamma_i \leq \frac{1}{4}$ for all $i \in \mathbb{N}$ and $\gamma_j < \frac{1}{4}$ for at least one $j \in \mathbb{N}$, and hence $\sum_{i=1}^{\infty} (\frac{1}{2})^i \cdot \gamma_i < \frac{1}{4}$. Therefore the two-counter machine does not halt if and only if there exists a strategy in the constructed cdPTA that reaches the target locations with probability at least $\frac{1}{4}$, concluding the proof of Theorem 1. □

4 Approximation of Reachability Probabilities

We now consider the approximation of maximal and minimal reachability probabilities of cdPTA. Our approach is to utilise concepts from the corner-point abstraction [10]. Recall that the standard corner-point abstraction is a finite-state system that extends the classical region graph by encoding regions and corner points within its states; for example, the state $(l, 0 < x < 1, x = 1)$ represents the situations in which the system is in location l, and the value of the clock x is in the interval $(0, 1)$ and is "close" to 1. The corner-point abstraction can be used to obtain a quantitative measure that is arbitrarily close to the actual one; this is typical in the context of weighted (or priced) timed automata (see [17] for a survey). Instead, in the context of cdPTA, as indicated by Example 2 and the undecidability results presented in Section 3, such a construction cannot be used directly to obtain maximal or minimal reachability probabilities that are arbitrarily close to those of the cdPTA under consideration. Hence we present a method that conservatively *approximates* maximal and minimal reachability probabilities (i.e., the computed maximal probability bounds the actual maximal probability from above, and the computed minimal probability bounds the actual minimal probability from below), and show that successive refinement of regions leads to finite-state systems that approximate the actual maximal and minimal probabilities at least as accurately. The states of our finite-state system correspond to location-region pairs, rather than to location-region-corner point triples as in the standard corner-point abstraction, and we use corners of regions only to define available distributions.

First we define regions and corner points. Let $\mathcal{P} = (L, \bar{l}, \mathcal{X}, inv, prob)$ be a cdPTA, which we assume to be fixed throughout this section, and let $M \in \mathbb{N}$ denote the upper bound on clocks in $\mathcal{P}$. We choose $k \in \mathbb{N}$, which we will refer to as the *(time) granularity*, and let

$[k] = \{\frac{c}{k} : c \in \mathbb{N}\}$ be the set of multiples of $\frac{1}{k}$. A *k-region* $(h, [X_0, ..., X_n])$ over $\mathcal{X}$ comprises:

1. a function $h : \mathcal{X} \to ([k] \cap [0, M])$ assigning a multiple of $\frac{1}{k}$ no greater than M to each clock and
2. a partition $[X_0, ..., X_n]$ of $\mathcal{X}$, where $X_i \neq \emptyset$ for all $1 \leq i \leq n$ and $h(x) = M$ implies $x \in X_0$ for all $x \in \mathcal{X}$.

Given clock valuation $v \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$ such that $v(x) \leq M$ for all $x \in \mathcal{X}$, and granularity k, the *k-region* $R = (h, [X_0, ..., X_n])$ *containing* v, written $v \in R$, satisfies the following conditions:

1. $\lfloor k \cdot v(x) \rfloor = k \cdot h(x)$ for all clocks $x \in \mathcal{X}$;
2. $v(x) = h(x)$ for all clocks $x \in X_0$;
3. $k \cdot v(x) - \lfloor k \cdot v(x) \rfloor \leq k \cdot v(y) - \lfloor k \cdot v(y) \rfloor$ if and only if $x \in X_i$ and $y \in X_j$ with $i \leq j$, for all clocks $x, y \in \mathcal{X}$.

Note that, rather than considering regions delimited by valuations corresponding to natural numbers, in our definition regions are delimited by valuations corresponding to multiples of $\frac{1}{k}$. We use Regs_k to denote the set of k-regions. For $R, R' \in \mathsf{Regs}_k$ and clock constraint $\psi \in CC(\mathcal{X})$, we say that R' is a *ψ-satisfying time successor* of R if, for all $v \in R$, there exists $\delta \in \mathbb{R}_{\geq 0}$, such that $(v+\delta) \in R'$ and $(v+\delta') \models \psi$ for all $0 \leq \delta' \leq \delta$. We write $R \models \psi$ if all valuations $v \in R$ are such that $v \models \psi$ (note that the definition of k-regions implies that either $v \models \psi$ for all $v \in R$ or $v \not\models \psi$ for all $v \in R$). For a given k-region $R \in \mathsf{Regs}_k$, we let $R[X := 0]$ be the k-region that corresponds to resetting clocks in X to 0 from clock valuations in R (that is, $R[X := 0]$ contains valuations $v[X := 0]$ for $v \in R$). We use $R_{\mathbf{0}}$ to denote the k-region that contains the valuation $\mathbf{0}$.

A *corner point* $\alpha = \langle a_i \rangle_{0 \leq i \leq n} \in ([k] \cap [0, M])^n$ of k-region $(h, [X_0, ..., X_n])$ is defined by:

$$a_i(x) = \begin{cases} h(x) & \text{if } x \in X_j \text{ with } j \leq i \\ h(x) + \frac{1}{k} & \text{if } x \in X_j \text{ with } j > i \ . \end{cases}$$

Note that a k-region $(h, [X_0, ..., X_n])$ is associated with $n+1$ corner points. Let $\mathsf{CP}(R)$ be the set of corner points of k-region R. Given granularity k, we let $\mathsf{CornerPoints}_k$ be the set of all corner points of k-regions.

Next we define the *clock-dependent region graph with granularity k* as the finite-state PTS $\mathcal{A}_k = (\mathsf{S}_k, \bar{\mathsf{s}}, \mathsf{Act}_k, \Gamma_k)$, where $\mathsf{S}_k = L \times \mathsf{Regs}_k$, $\bar{\mathsf{s}} = (\bar{l}, R_{\mathbf{0}})$, $\mathsf{Act}_k = \{\tau\} \cup (\mathsf{CornerPoints}_k \times \mathit{prob})$, and $\Gamma_k = \overrightarrow{\Gamma_k} \cup \widehat{\Gamma_k}$ where $\overrightarrow{\Gamma_k} \subseteq \mathsf{S}_k \times \{\tau\} \times \mathsf{Dist}(\mathsf{S}_k)$ and $\widehat{\Gamma_k} \subseteq \mathsf{S}_k \times \mathsf{CornerPoints}_k \times \mathit{prob} \times \mathsf{Dist}(\mathsf{S}_k)$ are such that:

- $\overrightarrow{\Gamma_k}$ is the smallest set of transitions such that $((l, R), \tau, \{(l, R') \mapsto 1\}) \in \overrightarrow{\Gamma_k}$ if (l, R') is an $\mathit{inv}(l)$-satisfying time successor of (l, R);
- $\widehat{\Gamma_k}$ is the smallest set such that $((l, R), (\alpha, (l, g, \mathfrak{p})), \nu) \in \widehat{\Gamma_k}$ if:
  1. $R \models g$;
  2. $\alpha \in \mathsf{CP}(R)$;
  3. for any $(l', R') \in \mathsf{S}_k$, we have that $\nu(l', R') = \sum_{X \in \mathsf{Reset}(R, R')} \mathfrak{p}[\alpha](X, l')$, where $\mathsf{Reset}(R, R') = \{X \subseteq \mathcal{X} \mid R[X := 0] = R'\}$.

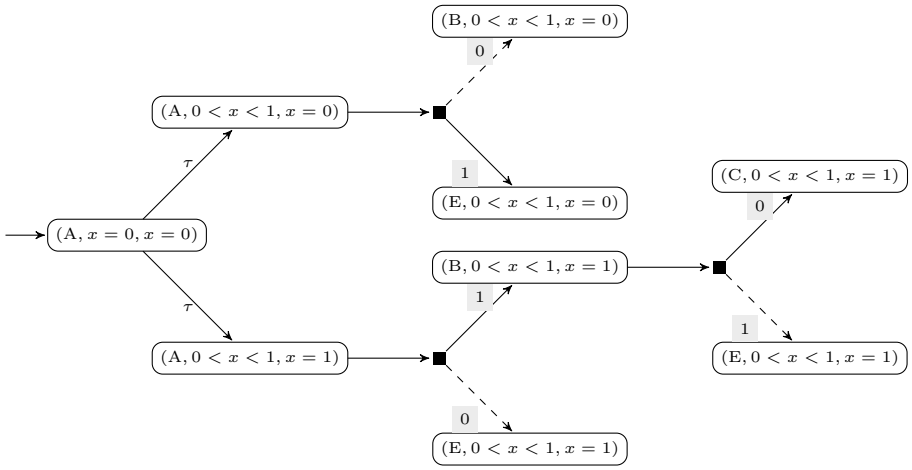

Figure 6: A finite-state PTS showing that a direct approach encoding corner points in states does not lead to a conservative overapproximation of the cdPTA with regard to reachability probabilities.

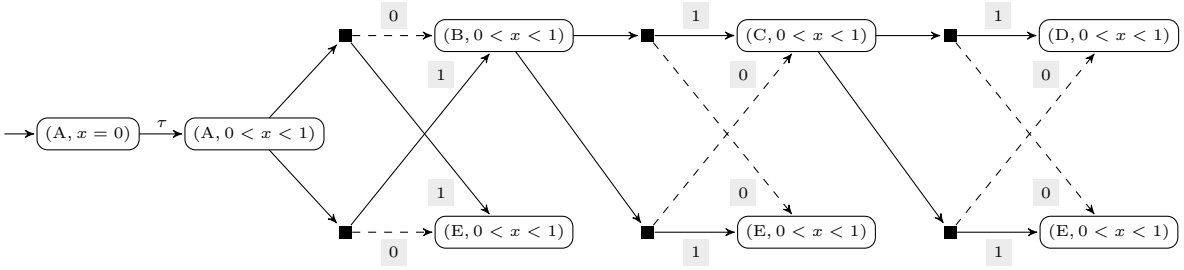

Figure 7: The clock-dependent region graph of Example 2 for $k = 1$.

Hence the clock-dependent region graph of a cdPTA encodes corner points within (probabilistic-edge-based) transitions, in contrast to the corner-point abstraction, which encodes corner points within states. In fact, a literal application of the standard corner-point abstraction, as presented in [17], does not result in a conservative approximation, which we now explain with reference to Example 2.

Example 3. *Recall that the states of the corner-point abstraction comprise a location, a region and a corner point of the region, and each transition maintains consistency between the corner points of the transition's source and target states. For example, for the cdPTA of Figure 2, consider the state* $(\mathrm{A}, 0 < x < 1, x = 1)$*, where* $0 < x < 1$ *is used to refer to the state's region component and* $x = 1$ *is used to refer to the state's corner point. Then the probabilistic edge leaving location* A *is enabled (because the state represents the situation in which clock* x *is in the interval* $(0, 1)$ *and arbitrarily close to* 1*). Standard intuition on the corner-point abstraction (adapted from weights in [17] to probabilities in distribution templates in this paper) specifies that, when considering probabilities of outgoing probabilistic edges, the state* $(\mathrm{A}, 0 < x < 1, x = 1)$ *should be associated with probabilities corresponding to the valuation for which* $x = 1$*. Hence the probability of making a transition to location* B *is* 1*, and the target corner-point-abstraction state is* $(\mathrm{B}, 0 < x < 1, x = 1)$*. However, now consider the probabilistic edge leaving location* B*: in this case, given that the corner point under consideration is* $x = 1$*, the probability of making a transition to location* C *is* 0*, and hence the target location* D *is reachable with probability* 0*. Furthermore, consider the state* $(\mathrm{A}, 0 < x < 1, x = 0)$*: in this case, if the probabilistic edge leaving location* A *is taken, then location* B *is reached with probability* 0*, and hence location* D *is again reachable with*

probability 0. *Following this approach of encoding corner points within states, we obtain the finite-state PTS in Figure 6. For emphasis, we show (with dashed lines) transitions that correspond to probability* 0*; vice versa, for simplicity we do not show transitions from states reached with probability* 0 *or from the location* E*, and duplicate the state* $(\mathrm{E}, 0 < x < 1, x = 1)$*. We can conclude that such a direct application of the corner-point abstraction to cdPTA is not a conservative approximation of the cdPTA, because the maximum probability of reaching location* D *in the corner-point abstraction is* 0*, i.e., less than the maximum probability of reaching location* D *in the cdPTA (which we recall is* $1 - \frac{\sqrt{3}}{3}$*).*

Instead, in our definition of the clock-dependent region graph, we allow "inconsistent" corner points to be used in successive transitions: for example, from location A*, the outgoing probabilistic edge can be taken using the value of* x *corresponding to the corner point* $x = 1$*; then, from locations* B *and* C*, the outgoing probabilistic edge can be taken using corner point* $x = 0$*. This approach, with* $k = 1$*, yields the finite-state PTS shown in Figure 7; as above, we show transitions with probability* 0 *with dashed lines, and for simplicity duplicate the state* $(\mathrm{E}, 0 < x < 1)$ *and omit self-loops labelled with* τ*. The distributions depicted in the top part of the figure correspond to the corner point with* $x = 0$*, whereas the distributions of the bottom part correspond to the corner point with* $x = 1$*. It can be observed that the maximum probability of reaching the target location* D *in this clock-dependent region graph is* 1 *(i.e., greater than* $1 - \frac{\sqrt{3}}{3}$*, as required by a conservative approximation approach).*

Analogously to the case of cdPTA strategies, we consider strategies of clock-dependent region graphs that alternate between transitions from $\overrightarrow{\Gamma_k}$ (time elapse transitions) and transitions from $\widehat{\Gamma_k}$ (probabilistic edge transitions). Formally, a *region graph strategy* π is a strategy of $\mathcal{A}_k$ such that, for a finite run $r \in \mathit{FinRuns}^{\mathcal{A}_k}$ that has $(l, R) \xrightarrow{a,\nu} (l', R')$ as its final transition, either $((l, R), a, \nu) \in \overrightarrow{\Gamma_k}$ and $\mathsf{support}(\pi(r)) \subseteq \widehat{\Gamma_k}$, or $((l, R), a, \nu) \in \widehat{\Gamma_k}$ and $\mathsf{support}(\pi(r)) \subseteq \overrightarrow{\Gamma_k}$. We write $\mathbf{\Pi}_k$ for the set of region graph strategies of $\mathcal{A}_k$.

Let $F \subseteq L$ be a set of target locations, which we assume to be fixed in the following. Recall that $S_F = \{(l, v) \in L \times \mathbb{R}^{\mathcal{X}}_{\geq 0} : l \in F\}$ and let $\mathsf{Regs}^F_k = \{(l, R) \in \mathsf{S}_k : l \in F\}$. The remainder of this section is dedicated to showing that clock-dependent region graphs can be used to provide a technique for approximating maximal and minimum probability for reaching target locations. We first show in Proposition 2 that, for any $k \geq 1$, the maximum (minimum) probability for reaching target locations from the initial state of a cdPTA is bounded from above (from below, respectively) by the corresponding maximum (minimum, respectively) probability in the clock-dependent region graph with granularity k. Then we show in Proposition 3 that, similarly, the maximum (minimum) probability computed in the clock-dependent region graph of granularity k is an upper (lower, respectively) bound on the maximum (minimum, respectively) probability computed in the clock-dependent region graph of granularity $2k$.

4.1 Approximating a cdPTA with a clock-dependent region graph

In this subsection, we show that we can use $\mathcal{A}_k$, the clock-dependent region graph with granularity k, to approximate the cdPTA $\mathcal{P}$. In order to show the required result, we first consider the following intermediate lemmata.

The first lemma specifies that the sets of clocks that, when reset to 0, are used to transform valuation v to valuation v' are the same as the sets of clocks used to transform the k-region containing v to the k-region containing the valuation v'.

Lemma 1. *Let* $k \in \mathbb{N}$ *and* $v, v' \in \mathbb{R}^{\mathcal{X}}_{\geq 0}$ *such that, for each clock* $x \in \mathcal{X}$*, either* $v'(x) = v(x)$ *or* $v'(x) = 0$*. Using* $R, R' \in \mathsf{Regs}_k$ *to denote the* k*-regions such that* $v \in R$ *and* $v' \in R'$*, we have* $\mathsf{Reset}(v, v') = \mathsf{Reset}(R, R')$*.*

Proof. Let X_v^0 be the set of clocks that are equal to 0 in v, and let $X_{v'}^0$ be the set of clocks that are equal to 0 in v'. Similarly, let X_R^0 be the set of clocks that are equal to 0 in all valuations in R, and let $X_{R'}^0$ be the set of clocks that are equal to 0 in all valuations in R'. By the definition of k-regions, for any clock $x \in \mathcal{X}$, we have $v(x) = 0$ if and only if $v''(x) = 0$ for all $v'' \in R$, and $v'(x) = 0$ if and only if $v''(x) = 0$ for all $v'' \in R'$. Hence $X_v^0 = X_R^0$ and $X_{v'}^0 = X_{R'}^0$. Given that either $v'(x) = v(x)$ or $v'(x) = 0$ for each $x \in \mathcal{X}$, we have that $X \in \mathsf{Reset}(v, v')$ if and only if $X_{v'}^0 \setminus X_v^0 \subseteq X \subseteq X_{v'}^0$. Similarly, $X \in \mathsf{Reset}(R, R')$ if and only if $X_{R'}^0 \setminus X_R^0 \subseteq X \subseteq X_{R'}^0$. Therefore we have that $X \in \mathsf{Reset}(v, v')$ if and only if $X_{v'}^0 \setminus X_v^0 \subseteq X \subseteq X_{v'}^0$ if and only if $X_{R'}^0 \setminus X_R^0 \subseteq X \subseteq X_{R'}^0$ if and only if $X \in \mathsf{Reset}(R, R')$. Hence $\mathsf{Reset}(v, v') = \mathsf{Reset}(R, R')$. □

Recall that we denote a set of weights by a finite set $\{\theta_i\}_{i \in I}$, where $\theta_i \in (0, 1]$ for each $i \in I$ and $\sum_{i \in I} \theta_i = 1$. In the following, we use an interpretation of valuations and corner points as points in $\mathbb{R}_{\geq 0}^{|\mathcal{X}|}$-space, allowing the use of operations such as $\theta \cdot v$ and $v + v'$ (interpreted as $(\theta \cdot v)(x) = \theta \cdot v(x)$ and $(v + v')(x) = v(x) + v'(x)$ for all clocks $x \in \mathcal{X}$, respectively).

Lemma 2. *Let $v \in \mathbb{R}_{\geq 0}^{\mathcal{X}}$, let $k \in \mathbb{N}$ and let $R \in \mathsf{Regs}_k$ be the unique k-region such that $v \in R$. Then there exists a set of weights $\{\theta_\alpha\}_{\alpha \in \mathsf{CP}(R)}$ such that $v = \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \alpha$.*

Proof. Observe that the convex hull of corner points $\mathsf{CP}(R)$ corresponds to a superset of the valuations contained in R. Hence, given that $v \in R$, we have that v is in the set of valuations induced by the convex hull of $\mathsf{CP}(R)$, and hence there exists $\{\theta_\alpha\}_{\alpha \in \mathsf{CP}(R)}$ with the required property. □

In the following, for a state $(l, v) \in S$ of $[\![\mathcal{P}]\!]$, we use $\langle\!\langle l, v \rangle\!\rangle_k$ to denote the unique pair $(l', R) \in L \times \mathsf{Regs}_k$ such that $l = l'$ and $v \in R$.

Lemma 3. *Let $(l, v) \in S$ be a state, let $k \in \mathbb{N}$, let $R \in \mathsf{Regs}_k$ be the k-region such that $v \in R$, and let $(l, g, \mathfrak{p}) \in prob$ be a probabilistic edge such that $v \models g$. Then there exists a set of weights $\{\theta_\alpha\}_{\alpha \in \mathsf{CP}(R)}$ such that, for any $(X, l') \in 2^{\mathcal{X}} \times L$:*

$$\mathfrak{p}[v](X, l') = \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \mathfrak{p}[\alpha](X, l') \; .$$

Proof. Let $\{\theta_\alpha\}_{\alpha \in \mathsf{CP}(R)}$ be the set of weights such that $v = \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \alpha$, which exists by Lemma 2. Let $e = (X, l') \in 2^{\mathcal{X}} \times L$. Then we have:

$$\begin{aligned}
\mathfrak{p}[v](e) &= \sum_{x \in \mathcal{X}} f_x^{p,e}(v(x)) \\
&= \sum_{x \in \mathcal{X}} (c_x^{p,e} + d_x^{p,e} \cdot v(x)) \\
&= \sum_{x \in \mathcal{X}} (c_x^{p,e} + d_x^{p,e} \cdot \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \alpha(x)) \\
&= \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \sum_{x \in \mathcal{X}} d_x^{p,e} \cdot \alpha(x) \quad (\text{from} \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha = 1) \\
&= \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha (\sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{x \in \mathcal{X}} d_x^{p,e} \cdot \alpha(x)) \; .
\end{aligned}$$

Recall that I_x^p has natural-numbered endpoints, and that $\alpha(x)$ is a rational number. Note that I_x^p may not include $\alpha(x)$ in the case that I_x^p is open or half-open. Given that $f_x^{p,e}$ is a continuous function, we have that $f_x^{p,e}(\gamma) = c_x^{p,e} + d_x^{p,e} \cdot \gamma$ for all γ in the closure of I_x^p. Given

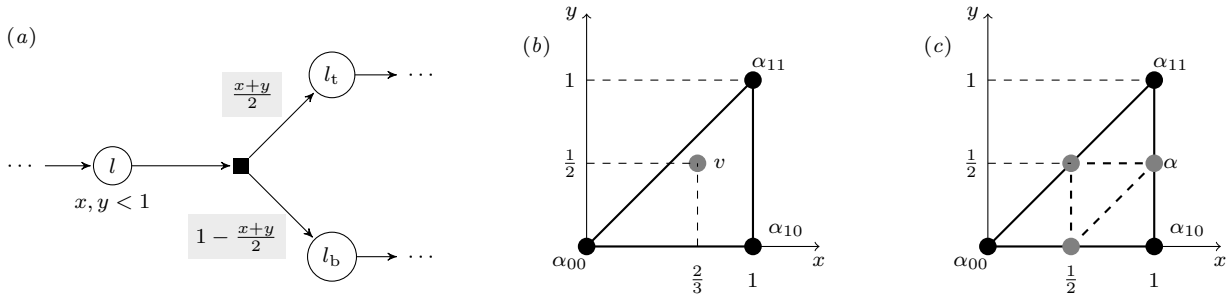

Figure 8: (a) The cdPTA fragment of Example 4. (b) 1-region for $x, y \in (0,1)$ and $y < x$, and valuation v with $v(x) = \frac{2}{3}$ and $v(y) = \frac{1}{2}$. (c) 1-region for $x, y \in (0,1)$ and $y < x$, and 2-regions contained within the 1-region.

that $\alpha(x)$ must belong to the closure of I_x^p, we conclude the following:

$$\begin{aligned}\sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \Big(\sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{x \in \mathcal{X}} d_x^{p,e} \cdot \alpha(x)\Big) &= \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \sum_{x \in \mathcal{X}} f_x^{p,e}(\alpha(x)) \\ &= \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \mathfrak{p}[\alpha](e)\ .\end{aligned}$$

Hence we have shown that $\mathfrak{p}[v](e) = \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \mathfrak{p}[\alpha](e)$, which concludes the proof. □

Example 4. *We illustrate Lemma 2 and Lemma 3 with regard to the cdPTA fragment shown in Figure 8(a), where the cdPTA has two clocks, x and y. Consider the state (l, v), i.e., the state for which the cdPTA is in location l with valuation v, where $v(x) = \frac{2}{3}$ and $v(y) = \frac{1}{2}$. The valuation v and the unique 1-region (which is characterised by $x, y \in (0,1)$ and $y < x$) containing v are shown in Figure 8(b). The corner points of the 1-region are α_{00}, α_{10} and α_{11}, where $\alpha_{00}(x) = \alpha_{00}(y) = 0$, $\alpha_{10}(x) = 1$ and $\alpha_{10}(y) = 0$, and $\alpha_{11}(x) = \alpha_{11}(y) = 1$. Now consider Lemma 2. The weights $\theta_{\alpha_{00}} = \frac{1}{3}$, $\theta_{\alpha_{10}} = \frac{1}{6}$, and $\theta_{\alpha_{11}} = \frac{1}{2}$ correspond to v, from the following reasoning:*

$$\begin{aligned}(\theta_{\alpha_{00}} \cdot \alpha_{00} + \theta_{\alpha_{10}} \cdot \alpha_{10} + \theta_{\alpha_{11}} \cdot \alpha_{11})(x) &= \theta_{\alpha_{00}} \cdot \alpha_{00}(x) + \theta_{\alpha_{10}} \cdot \alpha_{10}(x) + \theta_{\alpha_{11}} \cdot \alpha_{11}(x) \\ &= \tfrac{1}{3} \cdot 0 + \tfrac{1}{6} \cdot 1 + \tfrac{1}{2} \cdot 1 = \tfrac{2}{3} = v(x)\ , \\ (\theta_{\alpha_{00}} \cdot \alpha_{00} + \theta_{\alpha_{10}} \cdot \alpha_{10} + \theta_{\alpha_{11}} \cdot \alpha_{11})(y) &= \theta_{\alpha_{00}} \cdot \alpha_{00}(y) + \theta_{\alpha_{10}} \cdot \alpha_{10}(y) + \theta_{\alpha_{11}} \cdot \alpha_{11}(y) \\ &= \tfrac{1}{3} \cdot 0 + \tfrac{1}{6} \cdot 0 + \tfrac{1}{2} \cdot 1 = \tfrac{1}{2} = v(y)\ .\end{aligned}$$

Next, we consider Lemma 3, and use $\mathfrak{p}$ to denote the probabilistic edge from location l. First note that $\mathfrak{p}[v](\emptyset, l_{\mathrm{t}}) = \frac{1}{2} \cdot (v(x) + v(y)) = \frac{1}{2} \cdot (\frac{2}{3} + \frac{1}{2}) = \frac{7}{12}$, and $\mathfrak{p}[v](\emptyset, l_{\mathrm{b}}) = 1 - \frac{1}{2} \cdot (v(x) + v(y)) = \frac{5}{12}$. Now considering the corner points, we have:

$$\begin{array}{lcllcll}
\mathfrak{p}[\alpha_{00}](\emptyset, l_{\mathrm{t}}) & = & \frac{1}{2} \cdot (\alpha_{00}(x) + \alpha_{00}(y)) & = & \frac{1}{2} \cdot (0+0) & = & 0\ , \\
\mathfrak{p}[\alpha_{00}](\emptyset, l_{\mathrm{b}}) & = & 1 - \frac{1}{2} \cdot (\alpha_{00}(x) + \alpha_{00}(y)) & = & 1 - \frac{1}{2} \cdot (0+0) & = & 1\ , \\
\mathfrak{p}[\alpha_{10}](\emptyset, l_{\mathrm{t}}) & = & \frac{1}{2} \cdot (\alpha_{10}(x) + \alpha_{10}(y)) & = & \frac{1}{2} \cdot (1+0) & = & \frac{1}{2}\ , \\
\mathfrak{p}[\alpha_{10}](\emptyset, l_{\mathrm{b}}) & = & 1 - \frac{1}{2} \cdot (\alpha_{10}(x) + \alpha_{10}(y)) & = & 1 - \frac{1}{2} \cdot (1+0) & = & \frac{1}{2}\ , \\
\mathfrak{p}[\alpha_{11}](\emptyset, l_{\mathrm{t}}) & = & \frac{1}{2} \cdot (\alpha_{11}(x) + \alpha_{11}(y)) & = & \frac{1}{2} \cdot (1+1) & = & 1\ , \\
\mathfrak{p}[\alpha_{11}](\emptyset, l_{\mathrm{b}}) & = & 1 - \frac{1}{2} \cdot (\alpha_{11}(x) + \alpha_{11}(y)) & = & 1 - \frac{1}{2} \cdot (1+1) & = & 0\ .
\end{array}$$

We conclude Example 4 by observing that the equality of Lemma 3 holds:

$$\begin{array}{rcl}
\sum_{\alpha\in\mathsf{CP}(\langle\!\langle l,v\rangle\!\rangle_1)}\theta_\alpha\cdot\mathfrak{p}[\alpha](\emptyset,l_\mathrm{t}) &=& \theta_{\alpha_{00}}\cdot\mathfrak{p}[\alpha_{00}](\emptyset,l_\mathrm{t})+\theta_{\alpha_{10}}\cdot\mathfrak{p}[\alpha_{10}](\emptyset,l_\mathrm{t})+\theta_{\alpha_{11}}\cdot\mathfrak{p}[\alpha_{11}](\emptyset,l_\mathrm{t})\\
&=& \frac{1}{3}\cdot 0+\frac{1}{6}\cdot\frac{1}{2}+\frac{1}{2}\cdot 1\\
&=& \frac{7}{12}\\
&=& \mathfrak{p}[v](\emptyset,l_\mathrm{t})\ ,\\
\sum_{\alpha\in\mathsf{CP}(\langle\!\langle l,v\rangle\!\rangle_1)}\theta_\alpha\cdot\mathfrak{p}[\alpha](\emptyset,l_\mathrm{b}) &=& \theta_{\alpha_{00}}\cdot\mathfrak{p}[\alpha_{00}](\emptyset,l_\mathrm{b})+\theta_{\alpha_{10}}\cdot\mathfrak{p}[\alpha_{10}](\emptyset,l_\mathrm{b})+\theta_{\alpha_{11}}\cdot\mathfrak{p}[\alpha_{11}](\emptyset,l_\mathrm{b})\\
&=& \frac{1}{3}\cdot 1+\frac{1}{6}\cdot\frac{1}{2}+\frac{1}{2}\cdot 0\\
&=& \frac{5}{12}\\
&=& \mathfrak{p}[v](\emptyset,l_\mathrm{b})\ .
\end{array}$$

We now use the previous three lemmata to show that, from a state (l,v) of the semantics of a cdPTA, a distribution derived from a particular probabilistic edge can be obtained as a weighted sum of distributions, derived from the same probabilistic edge, available at the corner points of the k-region containing (l,v).

Lemma 4. *Let $(l,v)\in S$ be a state, let $k\in\mathbb{N}$, and let $R\in\mathsf{Regs}_k$ be the k-region such that $v\in R$. For each transition $((l,v),(l,g,\mathfrak{p}),\mu)\in\widehat{\Delta}$ of $[\![\mathcal{P}]\!]$, there exists a set of transitions $\{(\langle\!\langle l,v\rangle\!\rangle_k,(\alpha,(l,g,\mathfrak{p})),\nu_\alpha)\}_{\alpha\in\mathsf{CP}(R)}\subseteq\widehat{\Gamma_k}$ of $\mathcal{A}_k$ and weights $\{\theta_\alpha\}_{\alpha\in\mathsf{CP}(R)}$ such that, for each state $(l',v')\in S$:*

$$\mu(l',v')=\sum_{\alpha\in\mathsf{CP}(R)}\theta_\alpha\cdot\nu_\alpha(\langle\!\langle l',v'\rangle\!\rangle_k)\ .$$

Proof. Let $\{\theta_\alpha\}_{\alpha\in\mathsf{CP}(R)}$ be the set of weights such that $v=\sum_{\alpha\in\mathsf{CP}(R)}\theta_\alpha\cdot\alpha$, which exists by Lemma 2, and let $R,R'\in\mathsf{Regs}_k$ be the k-regions such that $v\in R$ and $v'\in R'$. By definition of $[\![\mathcal{P}]\!]$, we have:

$$\begin{array}{rcll}
\mu(l',v') &=& \displaystyle\sum_{X\in\mathsf{Reset}(v,v')}\mathfrak{p}[v](X,l') & \\
&=& \displaystyle\sum_{X\in\mathsf{Reset}(v,v')}\sum_{\alpha\in\mathsf{CP}(R)}\theta_\alpha\cdot\mathfrak{p}[\alpha](X,l') & \text{(by Lemma 3)}\\
&=& \displaystyle\sum_{X\in\mathsf{Reset}(R,R')}\sum_{\alpha\in\mathsf{CP}(R)}\theta_\alpha\cdot\mathfrak{p}[\alpha](X,l') & \text{(by Lemma 1)}\\
&=& \displaystyle\sum_{\alpha\in\mathsf{CP}(R)}\theta_\alpha\sum_{X\in\mathsf{Reset}(R,R')}\mathfrak{p}[\alpha](X,l') & \\
&=& \displaystyle\sum_{\alpha\in\mathsf{CP}(R)}\theta_\alpha\cdot\nu_i(\langle\!\langle l',v'\rangle\!\rangle_k)\ . &
\end{array}$$

□

The next lemma specifies that any time elapse transition of $[\![\mathcal{P}]\!]$ can be mimicked by a transition of $\mathcal{A}_k$.

Lemma 5. *Let $(l,v)\in S$ be a state, and let $k\in\mathbb{N}$. For each transition $((l,v),\delta,\{(l,v+\delta)\mapsto 1\})\in\overrightarrow{\Delta}$ of $[\![\mathcal{P}]\!]$, there exists a transition $(\langle\!\langle l,v\rangle\!\rangle_k,\tau,\{\langle\!\langle l,v+\delta\rangle\!\rangle_k\mapsto 1\})\in\overrightarrow{\Gamma_k}$ of $\mathcal{A}_k$.*

Proof. The lemma follows directly from the definition of $\overrightarrow{\Gamma_k}$ and of $inv(l)$-satisfying time successors. □

The following lemma specifies that, for any transition of $[\![\mathcal{P}]\!]$, any two distinct states within its distribution's support set have valuations belonging to different k-regions.

Lemma 6. *Let $(l, v) \in S$ be a state, let $k \in \mathbb{N}$, and let $((l, v), (l, g, \mathfrak{p}), \mu) \in \widehat{\Delta}$ be a transition of $[\![\mathcal{P}]\!]$. For each pair $(l_1, v_1), (l_2, v_2) \in \mathsf{support}(\mu)$ such that $(l_1, v_1) \neq (l_2, v_2)$, we have $\langle\!|l_1, v_1|\!\rangle_k \neq \langle\!|l_2, v_2|\!\rangle_k$.*

Proof. Let $(l_1, v_1), (l_2, v_2) \in \mathsf{support}(\mu)$ such that $(l_1, v_1) \neq (l_2, v_2)$. First observe that if $l_1 \neq l_2$ then trivially $\langle\!|l_1, v_1|\!\rangle_k \neq \langle\!|l_2, v_2|\!\rangle_k$. Now consider the case in which $l_1 = l_2$ and $v_1 \neq v_2$. Note that the definition of $[\![\mathcal{P}]\!]$ specifies that $v_1 = v[X_1 := 0]$ and $v_2 = v[X_2 := 0]$ for some clock sets $X_1, X_2 \subseteq \mathcal{X}$ such that $X_1 \neq X_2$. Hence v_1 and v_2 differ only in terms of which clocks are equal to 0. Intuitively, by the definition of k-regions, any two valuations that differ only in terms of which clocks are equal to 0 belong to different k-regions. For completeness, we now explain this formally. Denote the sets of clocks that are equal to 0 in v_1 by X_1' and in v_2 by X_2' (note that $X_1 \subseteq X_1'$, $X_2 \subseteq X_2'$ and that $X_1' \neq X_2'$ because $v_1 \neq v_2$). Let the k-region component of $\langle\!|l_1, v_1|\!\rangle_k$ be denoted by $(h_1, [X_{1,0}, X_{1,1}, ..., X_{1,n_1}])$ and let the k-region component of $\langle\!|l_2, v_2|\!\rangle_k$ be denoted by $(h_2, [X_{2,0}, X_{2,1}, ..., X_{2,n_2}])$. Given that $X_1' \neq X_2'$, either there exists clock $x \in X_1' \setminus X_2'$ such that $h_1(x) = 0$ and $x \in X_{1,0}$ but either $h_2(x) \neq 0$ or $x \notin X_{2,0}$, or there exists clock $x \in X_2' \setminus X_1'$ such that $h_2(x) = 0$ and $x \in X_{2,0}$ but either $h_1(x) \neq 0$ or $x \notin X_{1,0}$. Hence we have either $h_1 \neq h_2$ or $X_{1,0} \neq X_{2,0}$, and therefore $\langle\!|l_1, v_1|\!\rangle_k \neq \langle\!|l_2, v_2|\!\rangle_k$. □

Lemma 6 specifies that, for each transition $((l, v), a, \mu) \in \Delta$ of $[\![\mathcal{P}]\!]$ and for each $(l', R) \in \mathsf{S}_k$, there exists at most one valuation $v' \in R$ such that $(l', v') \in \mathsf{support}(\mu)$. If such a valuation v' exists, we set $v_{\mu,(l',R)} = v'$, otherwise $v_{\mu,(l',R)}$ can be set to an arbitrary valuation. From this fact, together with Lemma 4 and Lemma 5, we obtain the following lemma.

Lemma 7. *Let $(l, v) \in S$ be a state, and let $k \in \mathbb{N}$. For each transition $((l, v), a, \mu) \in \Delta$ of $[\![\mathcal{P}]\!]$, there exists a combined transition $(\{(\langle\!|l, v|\!\rangle_k, a_i, \nu_i)\}_{i \in I}, \{\lambda_i\}_{i \in I})$ of $\mathcal{A}_k$ such that, for each $(l', R') \in \mathsf{S}_k$, we have:*

1. $\mu(l', v_{\mu,(l',R')}) = \sum_{i \in I} \lambda_i \cdot \nu_i(l', R')$;
2. $\sum_{v' \in R'} \mu(l', v') = \sum_{i \in I} \lambda_i \cdot \nu_i(l', R')$.

Proof. We first consider part (1). Let $R \in \mathsf{Regs}_k$ be the unique region such that $v \in R$. We consider the following two cases.

Case $a \in prob$. Let $p = a$. By Lemma 4, there exist $\{((l, R), (\alpha, p), \nu_\alpha)\}_{\alpha \in \mathsf{CP}(R)} \subseteq \widehat{\Gamma_k}$ of $\mathcal{A}_k$ and weights $\{\theta_\alpha\}_{\alpha \in \mathsf{CP}(R)}$ such that $\mu(l', v_{\mu,(l',R')}) = \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \nu_\alpha(\langle\!|l', v_{\mu,(l',R')}|\!\rangle_k)$. Hence we let $I = \mathsf{CP}(R)$ and $\lambda_\alpha = \theta_\alpha$ for each $\alpha \in \mathsf{CP}(R)$, concluding that $\mu(l', v_{\mu,(l',R')}) = \sum_{\alpha \in \mathsf{CP}(R)} \theta_\alpha \cdot \nu_\alpha(l', R') = \sum_{i \in I} \lambda_i \cdot \nu_i(l', R')$.

Case $a \in \mathbb{R}_{\geq 0}$. Let $\delta = a$. Note that, by definition of $[\![\mathcal{P}]\!]$, for the unique $(l', R') \in \mathsf{S}_k$ such that $l = l'$ and $v + \delta \in R'$, we must have $v_{\mu,(l',R')} = v + \delta$, i.e., $\mu(l', v_{\mu,(l',R')}) = \mu(l', v + \delta) = 1$. By Lemma 5, there exists $((l, R), \tau, \{\langle\!|l, v + \delta|\!\rangle_k \mapsto 1\}) \in \overrightarrow{\Gamma_k}$: hence we let $|I| = 1$ and let $\{\lambda_i\}_{i \in I}$ be the set containing a single weight equal to 1. Then we conclude that $\mu(l', v_{\mu,(l',R')}) = \mu(l', v + \delta) = 1 = \{\langle\!|l, v + \delta|\!\rangle_k \mapsto 1\}(\langle\!|l, v + \delta|\!\rangle_k) = \sum_{i \in I} \lambda_i \cdot \nu_i(l', R')$.

Part (2) of the lemma then follows from part (1) and Lemma 6, which establishes that $\sum_{v'' \in R'} \mu(l', v'') = \mu(l', v_{\mu,(l',R')})$ for $(l', R') \in \mathsf{S}_k$ such that there exists a valuation $v' \in R'$ with $(l', v') \in \mathsf{support}(\mu)$. □

Consider equivalence $\equiv \subseteq (S \uplus \mathsf{S}_k)^2$ over the states of the disjoint union of $[\![\mathcal{P}]\!]$ and $\mathcal{A}_k$ defined as the smallest equivalence satisfying the following conditions:

- for states $(l, v), (l', v') \in S$, we have $(l, v) \equiv (l', v')$ if $\langle\!|l, v|\!\rangle_k = \langle\!|l', v'|\!\rangle_k$ (i.e., $l = l'$, and v and v' belong to the same k-region in Regs_k);

- for $(l, v) \in S$, $(l', R) \in \mathsf{S}_k$, we have $(l, v) \equiv (l', R)$ if $\langle\!|l, v|\!\rangle_k = (l', R)$ (i.e., $l = l'$ and v belongs to R).

Then the following corollary is a direct consequence of part (2) of Lemma 7.

Corollary 1. *Let $(l, v) \in S$ be a state, and let $k \in \mathbb{N}$. For each transition $((l, v), a, \mu) \in \Delta$ of $[\![\mathcal{P}]\!]$, there exists a combined transition $(\{(\langle\!|l, v|\!\rangle_k, a_i, \nu_i)\}_{i \in I}, \{\lambda_i\}_{i \in I})$ of $\mathcal{A}_k$ such that $\mu \equiv \bigoplus_{i \in I} \lambda_i \cdot \nu_i$ and either $a_i = \tau$ for all $i \in I$ if $a \in \mathbb{R}_{\geq 0}$, and $\{a_i\}_{i \in I} \subseteq \mathsf{CornerPoints}_k \times prob$ otherwise.*

We now state the main result of this section.

Proposition 2. *Let $k \in \mathbb{N}$. Then:*

$$\mathbb{P}^{\max}_{[\![\mathcal{P}]\!], \mathbf{\Sigma}}(S_F) \leq \mathbb{P}^{\max}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k), \quad \textit{and} \quad \mathbb{P}^{\min}_{[\![\mathcal{P}]\!], \mathbf{\Sigma}}(S_F) \geq \mathbb{P}^{\min}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k) \; .$$

Proof. Consider $\preceq \subseteq (S \uplus \mathsf{S}_k)^2$ such that $\preceq$ is the smallest relation satisfying the following property: for $(l, v) \in S$, $(l', R) \in \mathsf{S}_k$, we have $(l, v) \preceq (l', R)$ if $\langle\!|l, v|\!\rangle_k = (l', R)$. By Corollary 1, $\preceq$ is a probabilistic simulation respecting $\equiv$ and $\{\tau\} \cup \mathbb{R}_{\geq 0}$. Then, by Proposition 1, we have that $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!], \Sigma_{\mathbb{R}_{\geq 0}}}(S_F) \leq \mathbb{P}^{\max}_{\mathcal{A}_k, \Sigma_{\{\tau\}}}(\mathsf{Regs}^F_k)$ and $\mathbb{P}^{\min}_{[\![\mathcal{P}]\!], \Sigma_{\mathbb{R}_{\geq 0}}}(S_F) \geq \mathbb{P}^{\min}_{\mathcal{A}_k, \Sigma_{\{\tau\}}}(\mathsf{Regs}^F_k)$. Noting that $\mathbf{\Sigma} = \Sigma_{\mathbb{R}_{\geq 0}}$ and $\mathbf{\Pi}_k = \Sigma_{\{\tau\}}$, we have that $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!], \mathbf{\Sigma}}(S_F) \leq \mathbb{P}^{\max}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k)$ and $\mathbb{P}^{\min}_{[\![\mathcal{P}]\!], \mathbf{\Sigma}}(S_F) \geq \mathbb{P}^{\min}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k)$. □

4.2 Approximating a clock-dependent region graph with granularity $2k$ with a clock-dependent region graph with granularity k

In this subsection, we show that $\mathcal{A}_k$, the clock-dependent region graph with granularity k approximates $\mathcal{A}_{2k}$, the clock-dependent region graph with granularity $2k$. The results of this subsection can be adapted to hold for granularity ck rather than $2k$, for any $c \in \mathbb{N} \setminus \{0, 1\}$: we consider only the case of $c = 2$ for simplicity. Before presenting the main result on approximating the case of granularity $2k$ by that of granularity k, we consider a number of intermediate lemmata, which have similarities with the intermediate lemmata presented in Section 4.1.

For $2k$-region $R \in \mathsf{Regs}_{2k}$ and k-region $R' \in \mathsf{Regs}_k$, we write $R \subseteq R'$ if every valuation that is contained in R is also contained in R' (i.e., if $\{v \in \mathbb{R}^{\mathcal{X}}_{\geq 0} : v \in R\} \subseteq \{v \in \mathbb{R}^{\mathcal{X}}_{\geq 0} : v \in R'\}$). Note that, for a given $2k$-region $R \in \mathsf{Regs}_{2k}$ there is exactly one k-region $R' \in \mathsf{Regs}_k$ such that $R \subseteq R'$. In the following, given the $2k$-region R, we use $[R]_k$ to denote the unique k-region such that $R \subseteq [R]_k$. We now adapt Lemma 1 to the case of $2k$-regions and k-regions: that is, the sets of clocks that, when reset to 0, are used to transform $2k$-region R to $2k$-region R' are the same as the sets of clocks used to transform the k-region containing the $2k$-region R to the k-region containing the $2k$-region R'. The proof of the lemma proceeds in an analogous manner to that of Lemma 1, and is therefore omitted.

Lemma 8. *Let $k \in \mathbb{N}$ and let $R_{2k}, R'_{2k} \in \mathsf{Regs}_{2k}$ such that $R'_{2k} = R_{2k}[X := 0]$ for some $X \subseteq \mathcal{X}$. Using $R_k, R'_k \in \mathsf{Regs}_k$ to denote the unique k-regions such that $R_{2k} \subseteq R_k$ and $R'_{2k} \subseteq R'_k$, we have $\mathsf{Reset}(R_{2k}, R'_{2k}) = \mathsf{Reset}(R_k, R'_k)$.*

The following result specifies that every corner point of $R \in \mathsf{Regs}_{2k}$ is either a corner point of $[R]_k$ or can be obtained from a weighted combination of corner points of $[R]_k$.

Lemma 9. *Let $k \in \mathbb{N}$ and let $R \in \mathsf{Regs}_{2k}$. For each corner point $\alpha \in \mathsf{CP}(R)$, there exist a set of weights $\{\theta_{\alpha'}\}_{\alpha' \in \mathsf{CP}([R]_k)}$ such that $\alpha = \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \alpha'$.*

Proof. Note that the convex hull of corner points in $\mathsf{CP}([R]_k)$ is a superset of the convex hull of corner points in $\mathsf{CP}(R)$. Hence, any corner point $\alpha \in \mathsf{CP}(R)$ is in the set of valuations induced by the convex hull of $\mathsf{CP}([R]_k)$, and hence there exists the required $\{\theta_{\alpha'}\}_{\alpha' \in \mathsf{CP}([R]_k)}$ such that $\alpha = \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \alpha'$. □

We note that the corner points of $R \in \mathsf{Regs}_{2k}$ are either also corner points of the unique $R' \in \mathsf{Regs}_k$ such that $R \subseteq R'$, or they are mid-points of edges of the polyhedron induced by the convex hull of the corner points of R'.

Lemma 9 allows us to state the following lemma (which is an analogue of Lemma 3).

Lemma 10. *Let $k \in \mathbb{N}$, let $R \in \mathsf{Regs}_{2k}$, let $(l, g, \mathfrak{p}) \in prob$ be a probabilistic edge such that $R \models g$, and let $\alpha \in \mathsf{CP}(R)$ be a corner point of R. Then there exists a set of weights $\{\theta_{\alpha'}\}_{\alpha' \in \mathsf{CP}([R]_k)}$ such that, for any $(X, l') \in 2^{\mathcal{X}} \times L$, we have:*

$$\mathfrak{p}[\alpha](X, l') = \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \mathfrak{p}[\alpha'](X, l') \ .$$

Proof. By Lemma 9, it is possible that $\alpha \in \mathsf{CP}([R]_k)$, in which case we let $\theta_\alpha = 1$ and trivially we have:

$$\mathfrak{p}[\alpha](X, l') = \theta_\alpha \cdot \mathfrak{p}[\alpha](X, l') = \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \mathfrak{p}[\alpha'](X, l') \ .$$

Now consider the case in which $\alpha \notin \mathsf{CP}([R]_k)$. We proceed in a similar manner to the proof of Lemma 3. By Lemma 9, we have the existence of a set of weights $\{\theta_{\alpha'}\}_{\alpha' \in \mathsf{CP}([R]_k)}$ such that $\alpha = \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \alpha'$. Let $e = (X, l') \in 2^{\mathcal{X}} \times L$. Then we have:

$$\begin{aligned}
\mathfrak{p}[\alpha](e) &= \sum_{x \in \mathcal{X}} f_x^{p,e}(\alpha(x)) \\
&= \sum_{x \in \mathcal{X}} (c_x^{p,e} + d_x^{p,e} \cdot \alpha(x)) \\
&= \sum_{x \in \mathcal{X}} (c_x^{p,e} + d_x^{p,e} \cdot \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \alpha'(x)) \\
&= \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \sum_{x \in \mathcal{X}} d_x^{p,e} \cdot \alpha'(x) \\
&= \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} (\sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{x \in \mathcal{X}} d_x^{p,e} \cdot \alpha'(x)) \\
&= \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \sum_{x \in \mathcal{X}} f_x^{p,e}(\alpha'(x)) \\
&= \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \mathfrak{p}[\alpha'](e)
\end{aligned}$$

(where the fourth equation follows from $\sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} = 1$, and the penultimate equation follows from the fact that $f_x^{p,e}$ is a continuous function, as in the proof of Lemma 3), which concludes the proof. □

Example 5. *Recall the cdPTA example of Figure 8(a). In Figure 8(c), we show the 1-region corresponding to $x, y \in (0, 1)$ and $y < x$, together with the 2-regions contained within this 1-region. Consider Lemma 9, and recall this lemma specifies that the corner points of a 2-region are either corner points of the 1-region that it is contained within, or are equal to the weighted combination of corner points of that 1-region. As an example, take the corner point*

α such that $\alpha(x) = 1$ and $\alpha(y) = \frac{1}{2}$: denoting by α_{00}, α_{10} and α_{11} the three corner points of the 1-region defined as in Example 4, the weights $\theta_{\alpha_{00}} = 0$, $\theta_{\alpha_{10}} = \frac{1}{2}$, and $\theta_{\alpha_{11}} = \frac{1}{2}$ witness Lemma 9, i.e., $(\theta_{\alpha_{00}} \cdot \alpha_{00} + \theta_{\alpha_{10}} \cdot \alpha_{10} + \theta_{\alpha_{11}} \cdot \alpha_{11})(x) = \theta_{\alpha_{00}} \cdot \alpha_{00}(x) + \theta_{\alpha_{10}} \cdot \alpha_{10}(x) + \theta_{\alpha_{11}} \cdot \alpha_{11}(x) = 0 \cdot 0 + \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = 1 = \alpha(x)$, and $(\theta_{\alpha_{00}} \cdot \alpha_{00} + \theta_{\alpha_{10}} \cdot \alpha_{10} + \theta_{\alpha_{11}} \cdot \alpha_{11})(y) = \theta_{\alpha_{00}} \cdot \alpha_{00}(y) + \theta_{\alpha_{10}} \cdot \alpha_{10}(y) + \theta_{\alpha_{11}} \cdot \alpha_{11}(y) = 0 \cdot 0 + \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 1 = \frac{1}{2} = \alpha(y)$. Now consider Lemma 10. First note that $\mathfrak{p}[\alpha](\emptyset, l_{\mathrm{t}}) = \frac{1}{2} \cdot (\alpha(x) + \alpha(y)) = \frac{1}{2} \cdot (1 + \frac{1}{2}) = \frac{3}{4}$, and $\mathfrak{p}[v](\emptyset, l_{\mathrm{b}}) = 1 - \frac{1}{2} \cdot (\alpha(x) + \alpha(y)) = \frac{1}{4}$. Recall that, as explained in Example 4, $\mathfrak{p}[\alpha_{00}](\emptyset, l_{\mathrm{t}}) = 0$, $\mathfrak{p}[\alpha_{00}](\emptyset, l_{\mathrm{b}}) = 1$, $\mathfrak{p}[\alpha_{10}](\emptyset, l_{\mathrm{t}}) = \frac{1}{2}$, $\mathfrak{p}[\alpha_{10}](\emptyset, l_{\mathrm{b}}) = \frac{1}{2}$, $\mathfrak{p}[\alpha_{11}](\emptyset, l_{\mathrm{t}}) = 1$, $\mathfrak{p}[\alpha_{11}](\emptyset, l_{\mathrm{b}}) = 0$. Then the following shows that Lemma 10 holds:

$$\begin{aligned}
\theta_{\alpha_{00}} \cdot \mathfrak{p}[\alpha_{00}](\emptyset, l_{\mathrm{t}}) + \theta_{\alpha_{10}} \cdot \mathfrak{p}[\alpha_{10}](\emptyset, l_{\mathrm{t}}) + \theta_{\alpha_{11}} \cdot \mathfrak{p}[\alpha_{11}](\emptyset, l_{\mathrm{t}}) &= 0 \cdot 0 + \tfrac{1}{2} \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot 1 \\
&= \tfrac{3}{4} \\
&= \mathfrak{p}[\alpha](\emptyset, l_{\mathrm{t}}) \ , \\
\theta_{\alpha_{00}} \cdot \mathfrak{p}[\alpha_{00}](\emptyset, l_{\mathrm{b}}) + \theta_{\alpha_{10}} \cdot \mathfrak{p}[\alpha_{10}](\emptyset, l_{\mathrm{b}}) + \theta_{\alpha_{11}} \cdot \mathfrak{p}[\alpha_{11}](\emptyset, l_{\mathrm{b}}) &= 0 \cdot 1 + \tfrac{1}{2} \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot 0 \\
&= \tfrac{1}{4} \\
&= \mathfrak{p}[\alpha](\emptyset, l_{\mathrm{b}}) \ .
\end{aligned}$$

Lemma 11. *Let $k \in \mathbb{N}$ and $R \in \mathsf{Regs}_{2k}$. For each transition $((l, R), (\alpha, (l, g, \mathfrak{p})), \nu) \in \widehat{\Gamma_{2k}}$ of $\mathcal{A}_{2k}$, there exists a set of transitions $\{(l, [R]_k), (\alpha', (l, g, \mathfrak{p})), \nu_{\alpha'})\}_{\alpha' \in \mathsf{CP}([R]_k)} \subseteq \widehat{\Gamma_k}$ of $\mathcal{A}_k$ and weights $\{\theta_{\alpha'}\}_{\alpha' \in \mathsf{CP}([R]_k)}$ such that, for each state $(l', R') \in \mathsf{S}_{2k}$, we have:*

$$\nu(l', R') = \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \nu_{\alpha'}(l', [R']_k) \ .$$

Proof. We proceed in a similar manner to the proof of Lemma 4. Let $\{\theta_{\alpha'}\}_{\alpha' \in \mathsf{CP}([R]_k)}$ be the set of weights such that $\alpha = \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \alpha'$, which exists by Lemma 9. Then for each $(l', R') \in \mathsf{S}_{2k}$, by the definition of $\mathcal{A}_{2k}$, we have:

$$\begin{aligned}
\nu(l', R') &= \sum_{X \in \mathsf{Reset}(R, R')} \mathfrak{p}[\alpha](X, l') \\
&= \sum_{X \in \mathsf{Reset}(R, R')} \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \mathfrak{p}[\alpha'](X, l') && \text{(by Lemma 10)} \\
&= \sum_{X \in \mathsf{Reset}([R]_k, [R']_k)} \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \mathfrak{p}[\alpha'](X, l') && \text{(by Lemma 8)} \\
&= \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \sum_{X \in \mathsf{Reset}([R]_k, [R']_k)} \mathfrak{p}[\alpha'](X, l') \\
&= \sum_{\alpha' \in \mathsf{CP}([R]_k)} \theta_{\alpha'} \cdot \nu_i(l', [R']_k) \ .
\end{aligned}$$

□

The next lemma considers time-successor transitions of the region graphs for granularity k and $2k$: as it relies on standard non-probabilistic reasoning on the region graphs, we omit its proof.

Lemma 12. *Let $k \in \mathbb{N}$ and let $(l, R) \in \mathsf{S}_{2k}$ be a state of $\mathcal{A}_{2k}$. For each transition $((l, R), \tau, \{(l, R') \mapsto 1\}) \in \overrightarrow{\Gamma_{2k}}$ of $\mathcal{A}_{2k}$, there exists a transition $((l, [R]_k), \tau, \{(l', [R']_k) \mapsto 1\}) \in \overrightarrow{\Gamma_k}$ of $\mathcal{A}_k$.*

The following lemma is an analogue of Lemma 6, applied to the case of k-regions and $2k$-regions.

Lemma 13. *Let $(l, R) \in \mathsf{Regs}_{2k}$ be a state of the region graph with granularity $2k$, and let $((l, R), (\alpha, (l, g, \mathfrak{p})), \nu) \in \widehat{\Gamma_{2k}}$ be a transition of $\mathcal{A}_{2k}$. For each pair $(l_1, R_1), (l_2, R_2) \in \mathsf{support}(\nu)$ such that $(l_1, R_1) \neq (l_2, R_2)$, we have $(l_1, [R_1]_k) \neq (l_2, [R_2]_k)$.*

Proof. Let $(l_1, R_1), (l_2, R_2) \in \mathsf{support}(\nu)$ such that $(l_1, R_1) \neq (l_2, R_2)$. If $l_1 \neq l_2$ then trivially $(l_1, [R_1]_k) \neq (l_2, [R_2]_k)$. Now consider the case in which $l_1 = l_2$ and $R_1 \neq R_2$. Note that the definition of $\mathcal{A}_k$ specifies that $R_1 = R[X_1 := 0]$ and $R_2 = R[X_2 := 0]$ for some clock sets $X_1, X_2 \subseteq \mathcal{X}$ such that $X_1 \neq X_2$. Let X_1' and X_2' be the set of clocks that are equal to 0 in R_1 and R_2, respectively, and note that $X_1' \neq X_2'$. Then $[R_1]_k = (h_1, [X_{1,0}, X_{1,1}..., X_{1,n_1}])$ and $[R_2]_k = (h_2, [X_{2,0}, X_{2,1}..., X_{2,n_2}])$ have the following properties: either there exists clock $x \in X_1' \setminus X_2'$ such that $h_1(x) = 0$ and $x \in X_{1,0}$ but either $h_2(x) \neq 0$ or $x \notin X_{2,0}$, or there exists clock $x \in X_2' \setminus X_1'$ such that $h_2(x) = 0$ and $x \in X_{2,0}$ but either $h_1(x) \neq 0$ or $x \notin X_{1,0}$. Hence we have $(l_1, [R_1]_k) \neq (l_2, [R_2]_k)$. □

Given $((l, R), (\alpha, (l, g, \mathfrak{p})), \nu) \in \widehat{\Gamma_{2k}}$ and $(l', R') \in \mathsf{S}_k$, Lemma 13 specifies that there exists at most one $2k$-region R'' such that $(l', R'') \in \mathsf{support}(\nu)$ and $R'' \subseteq R'$. In the case in which such a $2k$-region R'' exists, we let $R_{\nu,(l',R')} = R''$, otherwise we can set $R_{\nu,(l',R')}$ be equal to an arbitrary $2k$-region. From this fact, together with Lemma 11 and Lemma 12, we obtain the following lemma. Its proof is similar to that of Lemma 7, and hence we omit it.

Lemma 14. *Let $(l, R) \in \mathsf{S}_k$ be a state of the region graph with granularity $2k$. For each transition $((l, R), (\alpha, (l, g, \mathfrak{p})), \nu) \in \widehat{\Gamma_{2k}}$ of $\mathcal{A}_{2k}$, there exists a combined transition $(\{(l, [R]_k, a_i, \nu_i)\}_{i \in I}, \{\lambda_i\}_{i \in I})$ of $\mathcal{A}_k$ such that, for each $(l', R') \in \mathsf{S}_k$, we have:*

1. $\nu(l', R_{\nu,(l',R')}) = \sum_{i \in I} \lambda_i \cdot \nu_i(l', R')$;
2. $\sum_{R'' \in \mathsf{Regs}_{2k} \text{ s.t. } [R'']_k = R'} \nu(l', R'') = \sum_{i \in I} \lambda_i \cdot \nu_i(l', R')$.

Consider equivalence $\equiv \subseteq (\mathsf{S}_{2k} \uplus \mathsf{S}_k)^2$ over the states of the disjoint union of $\mathcal{A}_{2k}$ and $\mathcal{A}_k$ defined as the smallest equivalence satisfying the following conditions:

- for states $(l, R), (l', R') \in \mathsf{S}_{2k}$, we have $(l, R) \equiv (l', R')$ if $l = l'$, and $[R]_k = [R']_k$ (i.e., R and R' are contained in the same k-region in Regs_k);
- for $(l, R) \in \mathsf{S}_{2k}$, $(l', R') \in \mathsf{S}_k$, $(l, R) \equiv (l', R')$ if $l = l'$ and $[R]_k = R'$ (i.e., R is contained in R').

We then obtain the following corollary from part (2) of Lemma 14.

Corollary 2. *Let $(l, R) \in \mathsf{S}_{2k}$ be a state of $\mathcal{A}_{2k}$. For each transition $((l, R), a, \nu) \in \Gamma_{2k}$ of $\mathcal{A}_{2k}$, there exists a combined transition $(\{(l, [R]_k), a_i, \nu_i)\}_{i \in I}, \{\lambda_i\}_{i \in I})$ of $\mathcal{A}_k$ such that $\nu \equiv \bigoplus_{i \in I} \lambda_i \cdot \nu_i$, $a_i = \tau$ for all $i \in I$ if $a = \tau$, and $\{a_i\}_{i \in I} \subseteq \mathsf{CornerPoints}_k \times prob$ otherwise.*

We now proceed to the principal result of this subsection, which shows that maximum and minimum reachability probabilities in $\mathcal{A}_k$ bound maximum and minimum reachability probabilities in $\mathcal{A}_{2k}$.

Proposition 3. *Let $k \in \mathbb{N}$. Then:*

$$\mathbb{P}^{\max}_{\mathcal{A}_{2k}, \mathbf{\Pi}_{2k}}(\mathsf{Regs}^F_{2k}) \leq \mathbb{P}^{\max}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k), \quad \text{and} \quad \mathbb{P}^{\min}_{\mathcal{A}_{2k}, \mathbf{\Pi}_{2k}}(\mathsf{Regs}^F_{2k}) \geq \mathbb{P}^{\min}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k) \ .$$

Proof. Consider the relation $\preceq \subseteq (\mathsf{S}_{2k} \uplus \mathsf{S}_k)^2$ such that $\preceq$ is the smallest relation satisfying: for $(l, R) \in \mathsf{S}_{2k}$, $(l', R') \in \mathsf{S}_k$, $(l, R) \preceq (l', R')$ if $(l, [R]_k) = (l', R')$. By Corollary 2, we have that $\preceq$ is a probabilistic simulation respecting $\equiv$ and $\{\tau\}$. Then, by Proposition 1, we have that:

$$\begin{aligned} \mathbb{P}^{\max}_{\mathcal{A}_{2k}, \Sigma^{\mathcal{A}_{2k}}_{\{\tau\}}}(\mathsf{Regs}^F_{2k}) &\leq \mathbb{P}^{\max}_{\mathcal{A}_k, \Sigma^{\mathcal{A}_k}_{\{\tau\}}}(\mathsf{Regs}^F_k) \\ \mathbb{P}^{\min}_{\mathcal{A}_{2k}, \Sigma^{\mathcal{A}_{2k}}_{\{\tau\}}}(\mathsf{Regs}^F_{2k}) &\geq \mathbb{P}^{\min}_{\mathcal{A}_k, \Sigma^{\mathcal{A}_k}_{\{\tau\}}}(\mathsf{Regs}^F_k) \ . \end{aligned}$$

Noting that $\mathbf{\Pi}_{2k} = \Sigma^{\mathcal{A}_{2k}}_{\{\tau\}}$ and $\mathbf{\Pi}_k = \Sigma^{\mathcal{A}_k}_{\{\tau\}}$, we have that $\mathbb{P}^{\max}_{\mathcal{A}_{2k}, \mathbf{\Pi}_{2k}}(\mathsf{Regs}^F_{2k}) \leq \mathbb{P}^{\max}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k)$ and $\mathbb{P}^{\min}_{\mathcal{A}_{2k}, \mathbf{\Pi}_{2k}}(\mathsf{Regs}^F_{2k}) \geq \mathbb{P}^{\min}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k)$. □

Proposition 2 and Proposition 3 suggest the following approach for maximal and minimal reachability problems of cdPTA. Consider a maximal reachability problem that involves deciding whether $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!], \mathbf{\Sigma}}(S_F) \trianglerighteq \lambda$. We proceed by first constructing the clock-dependent region graph for some granularity $k \in \mathbb{N}$. If $\mathbb{P}^{\max}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k) \not\trianglerighteq \lambda$, then we know from Proposition 2 that $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!], \mathbf{\Sigma}}(S_F) \not\trianglerighteq \lambda$. If, instead, $\mathbb{P}^{\max}_{\mathcal{A}_k, \mathbf{\Pi}_k}(\mathsf{Regs}^F_k) \trianglerighteq \lambda$, then we choose some $n \geq 1$, construct $\mathcal{A}_{2^n \cdot k}$ and check whether $\mathbb{P}^{\max}_{\mathcal{A}_{2^n \cdot k}, \mathbf{\Pi}_{2^n \cdot k}}(\mathsf{Regs}^F_{2^n \cdot k}) \trianglerighteq \lambda$. This process continues until we have either established that $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!], \mathbf{\Sigma}}(S_F) \not\trianglerighteq \lambda$ or we have run out of resources. A similar approach can be taken with minimal reachability problems.

4.3 Bounding the approximation error for a subclass of cdPTA

In this subsection we show that, for a particular class of cdPTA, we can identify a bound on the difference between the optimal (maximum or minimum) value computed on the clock-dependent region graph with granularity k and the corresponding optimal value of the cdPTA. Our results are based on the fact that we can quantify the maximum difference between the distributions used from states within a region and the distributions corresponding to corner points of that region. This allows us to show the existence of ϵ-bisimulation relations [18, 19] between MCs obtained from region graph strategies and cdPTA strategies. The level of approximation, given by $\epsilon \in [0, 1]$, is a product of $\frac{1}{k}$ and a constant that depends on the cdPTA. Then a result of [19] can be applied to show that difference between (i) the maximum (minimum, respectively) probability of reaching the target locations within a certain number b of transitions computed on the clock-dependent region graph with granularity k and (ii) the maximum (minimum, respectively) probability of reaching the target locations within b transitions in the cdPTA, has an upper bound of $1 - (1 - \epsilon)^b$.

In order to use the above approach in the context of reachability problems, which consider whether a target location is reached within *any* number of transitions, we restrict our attention to a particular subclass of cdPTA. Let $b \in \mathbb{N}$. A cdPTA $\mathcal{P}$ is *b-step-bounded* if all runs of $\mathcal{P}$ either do not reach the target locations at all or reach the target locations within b transitions; formally, for each infinite run $r \in \Diamond S_F$, there exists $i \leq b$ such that $r(i) \in S_F$. A sufficient condition for a cdPTA to be b-step-bounded for some $b \in \mathbb{N}$ is when (1) we require that the target set of locations is reached within a time deadline (known as *time-bounded reachability*), and (2) all cycles of the cdPTA correspond to the elapse of at least one time unit (known as *structural non-Zenoness* [20]). In particular, we note that this condition is satisfied by the cdPTA of Figure 1: the time deadline is encoded in the cdPTA by letting clock y measure the total amount of time elapsed and by making the location ✓ reachable only when $y \leq c_{\max}$, and all cycles of the cdPTA of Figure 1 require at least one time unit to elapse.

Let $\mathcal{P} = (L, \bar{l}, \mathcal{X}, \mathit{inv}, \mathit{prob})$ be a cdPTA, let $F \subseteq L$, and assume that $\mathcal{P}$ is b-step-bounded with respect to F. Recalling that $S_F = \{(l, v) \in S : l \in F\}$, and letting $\Diamond^{\leq b} S_F = \{r \in$

$\mathit{InfRuns}^{[\![\mathcal{P}]\!]} : \exists i \leq b \text{ s.t. } r(i) \in S_F\}$, we observe that $r \in \Diamond^{\leq b} S_F$ if and only if $r \in \Diamond S_F$, for any $r \in \mathit{InfRuns}^{[\![\mathcal{P}]\!]}$.

Given that the results of [19] are stated in terms of MCs, we need to reason about properties of MCs arising from cdPTA strategies and region graph strategies. In the following, we fix $k, b \in \mathbb{N}$, the b-step-bounded cdPTA $\mathcal{P} = (L, \bar{l}, \mathcal{X}, \mathit{inv}, \mathit{prob})$, and the set $F \subseteq L$ of target locations. Let $\sigma \in \mathbf{\Sigma}$ be a cdPTA strategy and let $s \in S$ be a state of $[\![\mathcal{P}]\!]$. Consider the MC $\mathcal{M}_s^\sigma = (\mathbf{S}, \bar{\mathbf{s}}, \mathbf{P}_s^\sigma)$, where $\mathbf{S} = \mathit{FinRuns}^\sigma(s)$ and $\bar{\mathbf{s}} = s$, and let $\mathbf{InfRuns}^\sigma(\bar{\mathbf{s}})$ be the set of sequences $\mathbf{s}_0\mathbf{s}_1\cdots$ such that $\mathbf{s}_0 = \bar{\mathbf{s}}$ and $\mathbf{P}_s^\sigma(\mathbf{s}_i, \mathbf{s}_{i+1}) > 0$ for each $i \in \mathbb{N}$. For $\mathbf{r} = \mathbf{s}_0\mathbf{s}_1\cdots$, where $\mathbf{r} \in \mathbf{InfRuns}^\sigma(\bar{\mathbf{s}})$, and $i \in \mathbb{N}$, let $\mathbf{r}(i) = \mathbf{s}_i$. Consider the bijection $f : \mathit{InfRuns}^\sigma(s) \to \mathbf{InfRuns}^\sigma(\bar{\mathbf{s}})$ such that $f(s_0 \xrightarrow{a_0,\mu_0} s_1 \xrightarrow{a_1,\mu_1} s_2 \cdots) = (s_0)(s_0 \xrightarrow{a_0,\mu_0} s_1)(s_0 \xrightarrow{a_0,\mu_0} s_1 \xrightarrow{a_1,\mu_1} s_2)\cdots$. Then we can define a probability measure $\mathbf{Pr}_s^\sigma$ over $\mathbf{InfRuns}^\sigma(\bar{\mathbf{s}})$ such that $\mathbf{Pr}_s^\sigma(\{f(r) : r \in E\}) = \Pr_s^\sigma(E)$ for any measurable set $E \subseteq \mathit{InfRuns}^\sigma(s)$. Now let $\mathbf{S}_F \subseteq \mathbf{S}$ be the smallest set such that $\mathbf{s} \in \mathbf{S}_F$ if $\mathit{last}(\mathbf{s}) \in S_F$ (recall that each state in $\mathbf{S}$ is a finite run from $\mathit{FinRuns}^{[\![\mathcal{P}]\!]}$), and let $\Diamond^{\leq b}\mathbf{S}_F = \{\mathbf{r} \in \mathbf{InfRuns}^\sigma : \exists i \leq b \text{ s.t. } \mathbf{r}(i) \in \mathbf{S}_F\}$. Note that $\Diamond^{\leq b}\mathbf{S}_F = \{f(r) : r \in \Diamond^{\leq b} S_F\}$, and hence $\mathbf{Pr}_s^\sigma(\Diamond^{\leq b}\mathbf{S}_F) = \Pr_s^\sigma(\Diamond^{\leq b} S_F)$.

We now recall a number of technical definitions from [18, 19]. Let $\mathcal{M} = (\mathbf{S}, \bar{\mathbf{s}}, \mathbf{P})$ be an MC with a countable state space, let $\mathcal{R} \subseteq \mathbf{S} \times \mathbf{S}$ be a binary relation on $\mathbf{S}$, and let $\epsilon \in [0, 1]$. For a set $\mathbf{S}' \subseteq \mathbf{S}$, we define $\mathcal{R}(\mathbf{S}')$ to be the set of states related to states in $\mathbf{S}'$ by $\mathcal{R}$; formally, $\mathcal{R}(\mathbf{S}') = \{\mathbf{s} \in \mathbf{S} : \exists \mathbf{s}' \in \mathbf{S}' \text{ s.t. } (\mathbf{s}, \mathbf{s}') \in \mathcal{R}\}$. Let $\mathbf{S}_F \subseteq \mathbf{S}$. A symmetric binary relation $\mathcal{R} \subseteq \mathbf{S} \times \mathbf{S}$ over $\mathbf{S}$ is an *ϵ-bisimulation* if $(\mathbf{s}_1, \mathbf{s}_2) \in \mathcal{R}$ implies that (1) $\mathbf{s}_1 \in \mathbf{S}_F$ if and only if $\mathbf{s}_2 \in \mathbf{S}_F$, and (2) $\mathbf{P}(\mathbf{s}_2, \mathcal{R}(\mathbf{S}')) \geq \mathbf{P}(\mathbf{s}_1, \mathbf{S}') - \epsilon$ for all sets $\mathbf{S}' \subseteq \mathbf{S}$.[4] The following result is a direct corollary of Theorem 2 and Theorem 4 of [19].

Proposition 4. *Let $\mathcal{M} = (\mathbf{S}, \bar{\mathbf{s}}, \mathbf{P})$ be an MC with a countable state space, let $\mathbf{S}_F \subseteq \mathbf{S}$, let $b \in \mathbb{N}$, and let $\epsilon \in [0, 1]$. If $\mathbf{s}_1, \mathbf{s}_2 \in \mathbf{S}$ are ϵ-bisimilar, then $|\mathbf{Pr}_{\mathbf{s}_1}^\sigma(\Diamond^{\leq b}\mathbf{S}_F) - \mathbf{Pr}_{\mathbf{s}_2}^\sigma(\Diamond^{\leq b}\mathbf{S}_F)| \leq 1 - (1-\epsilon)^b$.*

As in the case of PTSs, we can define the disjoint union of the two MCs $\mathcal{M}_1 = (\mathbf{S}_1, \bar{\mathbf{s}}_1, \mathbf{P}_1)$ and $\mathcal{M}_2 = (\mathbf{S}_2, \bar{\mathbf{s}}_2, \mathbf{P}_2)$ as the MC $(\mathbf{S}_1 \uplus \mathbf{S}_2, \_, \mathbf{P})$, where the initial state is irrelevant and is hence omitted, and $\mathbf{P}$ is defined in the following way: for $\mathbf{s}, \mathbf{s}' \in \mathbf{S}_1 \uplus \mathbf{S}_2$, if $\mathbf{s}, \mathbf{s}' \in \mathbf{S}_1$ then $\mathbf{P}(\mathbf{s}, \mathbf{s}') = \mathbf{P}_1(\mathbf{s}, \mathbf{s}')$, if $\mathbf{s}, \mathbf{s}' \in \mathbf{S}_2$ then $\mathbf{P}(\mathbf{s}, \mathbf{s}') = \mathbf{P}_2(\mathbf{s}, \mathbf{s}')$, otherwise $\mathbf{P}(\mathbf{s}, \mathbf{s}') = 0$.

We now proceed to explain the relevance of Proposition 4 to b-step-bounded cdPTA. First, we note that the combination of Corollary 1, Proposition 1 and [5, Theorem 8.6.1] implies that, for each cdPTA strategy $\sigma \in \mathbf{\Sigma}$ and each state $(l, v) \in S$ of $[\![\mathcal{P}]\!]$, we can obtain a region graph strategy $\pi \in \mathbf{\Pi}_k$ that mimics precisely the behaviour of σ from state (l, v), such that $\mathbf{Pr}_{(l,v)}^\sigma(\Diamond^{\leq b}\mathbf{S}_F) = \mathbf{Pr}_{\langle\!|(l,v)|\!\rangle_k}^\pi(\Diamond^{\leq b}\mathbf{S}_F)$. It remains to show that, for any region graph strategy $\pi \in \mathbf{\Pi}_k$, we can mimic π by a cdPTA strategy; however, it is not possible to mimic π precisely with a cdPTA strategy, and we have to settle for a cdPTA strategy that mimics π *approximately*. Our approach in the following is to define a cdPTA strategy $\sigma \in \mathbf{\Sigma}$ that defines an MC that is related to the MC induced by π by ϵ-bisimulation. Then, using Proposition 4, we conclude that the b-step-bounded reachability probabilities of σ and π do not exceed $1-(1-\epsilon)^b$.

A technical difficulty that arises in the construction of the cdPTA strategy σ is that σ may be forced to assign positive probability to some runs for which the associated runs of π assign probability 0 due to the fact that corner points can induce distributions assigning probability 0 to some outcomes. For example, in Figure 7, if the region strategy π chooses (with probability 1) the uppermost transition from $(\mathrm{A}, 0 < x < 1)$, then there is no run of π passing through $(\mathrm{B}, 0 < x < 1)$, because the corner point associated with the uppermost transition means that the probability of going to $(\mathrm{B}, 0 < x < 1)$ is 0. In contrast, for any cdPTA strategy, from

[4] Note that [19] requires $\mathbf{S}'$ be be measurable, which is implied in our context because we assume that $\mathcal{M}$ has a countable state space.

any state encoded by $(\mathrm{A}, 0 < x < 1)$, the outgoing probabilistic edge transition *must* assign probability greater than 0 to a state encoded by $(\mathrm{B}, 0 < x < 1)$. In order to obtain a 1-to-1 relationship between finite runs of π and the finite runs of the cdPTA strategy σ that we aim to construct, we modify the definition of the MC of π so that its state space also includes some finite runs that have probability 0.

Before presenting the modified MC, we require the following technical material. Let $(l, R) \in L \times \mathsf{Regs}_k$, and let $(l, g, \mathfrak{p}) \in \mathit{prob}$ such that $R \models g$. We define $\mathsf{support}[R](l, g, \mathfrak{p})$ as the set of outcomes that are assigned positive probability by $\mathfrak{p}$ from valuations within R. Formally, let $\mathsf{support}[R](l, g, \mathfrak{p}) = \{e \in 2^{\mathcal{X}} \times L : \exists v \in R \text{ s.t. } \mathfrak{p}[v](e) > 0\}$. Next, we identify the set of location-region pairs that are obtained from (l, R) by applying outcomes in $\mathsf{support}[R](l, g, \mathfrak{p})$. Formally, let $\mathsf{PT}((l, R), (l, g, \mathfrak{p})) = \{(l', R') \in L \times \mathsf{Regs}_k : (X, l') \in \mathsf{support}[R]((l, g, \mathfrak{p})) \text{ and } R' = R[X := 0]\}$ be the set of *potential targets* of (l, R) and $(l, g, \mathfrak{p})$.

A technical property that will be useful for subsequent proofs is that any outcome that is assigned positive probability by $\mathfrak{p}$ for *some* valuation in R is assigned positive probability by *all* valuations in R.

Lemma 15. *Let $(l, R) \in L \times \mathsf{Regs}_k$, let $(l, g, \mathfrak{p}) \in \mathit{prob}$ such that $R \models g$, and let $e \in 2^{\mathcal{X}} \times L$. If there exists $v \in R$ such that $\mathfrak{p}[v](e) > 0$ then $\mathfrak{p}[v'](e) > 0$ for all $v' \in R$.*

Proof. Aiming for a contradiction, assume that there exist valuations $v_{>0}, v_{=0} \in R$ such that $\mathfrak{p}[v_{>0}](e) > 0$ and $\mathfrak{p}[v_{=0}](e) = 0$. Using $(h, [X_0, ..., X_m])$ to denote R, let $\mathcal{X}_R^{\mathrm{o}} = \bigcup_{1 \leq i \leq m} X_i$ be the set of clocks that are not equal to a multiple of $\frac{1}{k}$ in R. Recall from Section 2.3 that $\mathfrak{p}[v'](e) = \sum_{x \in \mathcal{X}} f_x^{p,e}(v'(x)) \geq 0$ for all $v' \in R$. Let $\lambda = \sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{x \in \mathcal{X} \setminus \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{>0}(x)$. Note that $v_{>0}(x) = v_{=0}(x)$ for each $x \in \mathcal{X} \setminus \mathcal{X}_R^{\mathrm{o}}$, and hence $\sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{x \in \mathcal{X} \setminus \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{=0}(x) = \sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{x \in \mathcal{X} \setminus \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{>0}(x) = \lambda$.

Recall that, by definition, $\mathfrak{p}[v_{>0}](e) = \sum_{x \in \mathcal{X}} f_x^{p,e}(v_{>0}(x)) > 0$ and $\mathfrak{p}[v_{=0}](e) = \sum_{x \in \mathcal{X}} f_x^{p,e}(v_{=0}(x)) = 0$. We can write:

$$
\begin{aligned}
\mathfrak{p}[v_{>0}](e) &= \sum_{x \in \mathcal{X}} f_x^{p,e}(v_{>0}(x)) \\
&= \sum_{x \in \mathcal{X}} (c_x^{p,e} + d_x^{p,e} \cdot v_{>0}(x)) \\
&= \sum_{x \in \mathcal{X}} c_x^{p,e} + \sum_{x \in \mathcal{X} \setminus \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{>0}(x) + \sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{>0}(x) \\
&= \lambda + \sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{>0}(x) \ .
\end{aligned}
$$

Similarly, we can obtain $\mathfrak{p}[v_{=0}](e) = \lambda + \sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{=0}(x)$. Given that $\mathfrak{p}[v_{>0}](e) > 0$ and $\mathfrak{p}[v_{=0}](e) = 0$, we must have $\sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{>0}(x) > -\lambda$ and $\sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{=0}(x) = -\lambda$. Furthermore, for all $v' \in R$, we can conclude that $\sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v'(x) \geq -\lambda$ by similar reasoning and from the fact that $\mathfrak{p}[v'](e) \geq 0$. Now let $\mathcal{X}_R^{>0} = \{x \in \mathcal{X}_R^{\mathrm{o}} : d_x^{p,e} > 0\}$, let $\mathcal{X}_R^{<0} = \{x \in \mathcal{X}_R^{\mathrm{o}} : d_x^{p,e} < 0\}$, and let $\mathcal{X}_R^{=0} = \mathcal{X}_R^{\mathrm{o}} \setminus (\mathcal{X}_R^{>0} \cup \mathcal{X}_R^{<0})$. Note that it cannot be the case that $\mathcal{X}_R^{=0} = \mathcal{X}_R^{\mathrm{o}}$, because otherwise $d_x^{p,e} = 0$ for all $x \in \mathcal{X}_R^{\mathrm{o}}$, which would imply that both $\lambda > 0$ and $\lambda = 0$.

Let $\tilde{v} \in R$ be a valuation such that $h(x) < \tilde{v}(x) < v_{=0}(x)$ for each $x \in \mathcal{X}_R^{>0}$ and $v_{=0}(x) < \tilde{v}(x) < h(x) + \frac{1}{k}$ for each $x \in \mathcal{X}_R^{<0}$. Then we obtain $\sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot \tilde{v}(x) < \sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v_{=0}(x) = -\lambda$, which contradicts the fact that $\sum_{x \in \mathcal{X}_R^{\mathrm{o}}} d_x^{p,e} \cdot v'(x) \geq -\lambda$ for all $v' \in R$.

Overall, we have shown that there cannot exist $v_{>0}, v_{=0} \in R$ such that $\mathfrak{p}[v_{>0}](e) > 0$ and $\mathfrak{p}[v_{=0}](e) = 0$. The statement of the lemma then follows. □

The following lemma establishes that there is a 1-to-1 relationship between the target states of the cdPTA after taking a probabilistic edge and the potential targets of the region graph obtained after taking the same probabilistic edge.

Lemma 16. *Let* $((l,v),(l,g,\mathfrak{p}),\mu) \in \widehat{\Delta}$ *be a transition of* $[\![\mathcal{P}]\!]$*, and let* $\mathsf{support}(\mu) = \{(l_1,v_1),\ldots,(l_m,v_m)\}$*. Then* $\mathsf{PT}(\langle\!\langle l,v\rangle\!\rangle_k,(l,g,\mathfrak{p})) = \{\langle\!\langle l_1,v_1\rangle\!\rangle_k,\ldots,\langle\!\langle l_m,v_m\rangle\!\rangle_k\}$*, where* $\langle\!\langle l_i,v_i\rangle\!\rangle_k \neq \langle\!\langle l_j,v_j\rangle\!\rangle_k$ *for all* $i,j \in \{1,\ldots,m\}$ *such that* $i \neq j$*.*

Proof. First note that $\langle\!\langle l_i,v_i\rangle\!\rangle_k \neq \langle\!\langle l_j,v_j\rangle\!\rangle_k$ for all $i,j \in \{1,\ldots,m\}$ such that $i \neq j$ follows from Lemma 6.

Now we show that $\mathsf{PT}(\langle\!\langle l,v\rangle\!\rangle_k,(l,g,\mathfrak{p})) \supseteq \{\langle\!\langle l_1,v_1\rangle\!\rangle_k,\ldots,\langle\!\langle l_m,v_m\rangle\!\rangle_k\}$. Denote $\langle\!\langle l,v\rangle\!\rangle_k$ by (l,R) and $\langle\!\langle l_i,v_i\rangle\!\rangle_k$ by (l_i,R_i) (hence $v \in R$ and $v_i \in R_i$) for each $i \in \{1,\ldots,m\}$. Given that $(l_i,v_i) \in \mathsf{support}(\mu)$, we observe that $\mathfrak{p}[v](X,l_i) > 0$ and $v_i = v[X:=0]$ for some $X \subseteq \mathcal{X}$. From Lemma 1, we have $\mathsf{Reset}(v,v_i) = \mathsf{Reset}(R,R_i)$. Therefore $X \in \mathsf{Reset}(v,v_i)$ implies that $X \in \mathsf{Reset}(R,R_i)$. This in turn means that $R_i = R[X:=0]$. Hence $(l_i,R_i) \in \mathsf{PT}(\langle\!\langle l,v\rangle\!\rangle_k,(l,g,\mathfrak{p}))$.

Next, we show that $\mathsf{PT}(\langle\!\langle l,v\rangle\!\rangle_k,(l,g,\mathfrak{p})) \subseteq \{\langle\!\langle l_1,v_1\rangle\!\rangle_k,\ldots,\langle\!\langle l_m,v_m\rangle\!\rangle_k\}$. Let $(l',R') \in \mathsf{PT}(\langle\!\langle l,v\rangle\!\rangle_k,(l,g,\mathfrak{p}))$. Then, from the definition of potential targets and Lemma 15, we have that $R' = R[X:=0]$ and $\mathfrak{p}[v](X,l') > 0$ for some $X \subseteq \mathcal{X}$. Consider the valuation $v' = v[X:=0]$. Note that $v' \in R'$. The fact that $\mathfrak{p}[v](X,l') > 0$ means that $(l',v') \in \mathsf{support}(\mu)$, i.e., there exists $i \in \{1,\ldots,m\}$ such that $(l',v') = (l_i,v_i)$. Hence $(l',R') = \langle\!\langle l_i,v_i\rangle\!\rangle_k$. □

Given transition $((l,R),(\alpha,p),\nu) \in \widehat{\Gamma_k}$ we write $(l,R) \xrightarrow{(\alpha,p),\nu}\!\!\!\!\!\rightarrow (l',R')$ if (l',R') is a potential target of (l,R) and $(l,g,\mathfrak{p})$. A *potential finite run* is a finite sequence $(l_0,R_0) \xrightarrow{(\alpha_0,p_0),\nu_0}\!\!\!\!\!\rightarrow (l_1,R_1) \xrightarrow{(\alpha_1,p_1),\nu_1}\!\!\!\!\!\rightarrow \cdots \xrightarrow{(\alpha_{n-1},p_{n-1}),\nu_{n-1}}\!\!\!\!\!\rightarrow (l_n,R_n)$ and a *potential infinite run* is an infinite sequence $(l_0,R_0) \xrightarrow{(\alpha_0,p_0),\nu_0}\!\!\!\!\!\rightarrow (l_1,R_1) \xrightarrow{(\alpha_1,p_1),\nu_1}\!\!\!\!\!\rightarrow \cdots$. Let **PFinRuns** be the set of potential finite runs, and let $\mathbf{PFinRuns}(l,R)$ be the set of potential finite runs starting from (l,R). In the following, we assume that each region graph strategy $\pi \in \mathbf{\Pi}_k$ is a mapping from **PFinRuns** to $\mathsf{Dist}(\Gamma_k)$. The assumption allows us to define a 1-to-1 relationship between the potential runs of region graph strategies and the runs of constructed cdPTA strategies. Let $\mathbf{PFinRuns}^\pi(l,R)$ be the set of potential finite runs starting from (l,R) resulting from π (i.e., where each finite potential run $(\rho \xrightarrow{(\alpha,p),\nu}\!\!\!\!\!\rightarrow (l',R')) \in \mathbf{PFinRuns}^\pi(l,R)$ is such that $\pi(\rho)(last(\rho)(\alpha,p),\nu) > 0$). Then we define the *potential MC* of π and (l,R) as $\mathcal{M}^{\mathrm{Pot},\pi}_{(l,R)} = (\mathbf{PFinRuns}^\pi(l,R),(l,R),\mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)})$, where, for $\rho,\rho' \in \mathbf{PFinRuns}^\pi(l,R)$, we let $\mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho') = \pi(\rho)(last(\rho),(\alpha,p),\nu)\cdot\nu(l',R')$ if $\rho' = \rho \xrightarrow{(\alpha,p),\nu}\!\!\!\!\!\rightarrow (l',R')$, and $\mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho') = 0$ otherwise. We denote by $\mathbf{Pr}^{\mathrm{Pot},\pi}_{(l,R)}$ the probability measure associated with $\mathcal{M}^{\mathrm{Pot},\pi}_{(l,R)}$ over potential infinite runs. Note that, for finite run $(l_0,R_0) \xrightarrow{(\alpha_0,p_0),\nu_0} (l_1,R_1) \xrightarrow{(\alpha_1,p_1),\nu_1} \cdots \xrightarrow{(\alpha_{n-1},p_{n-1}),\nu_{n-1}} (l_n,R_n)$, there exists a unique potential finite run $(l_0,R_0) \xrightarrow{(\alpha_0,p_0),\nu_0}\!\!\!\!\!\rightarrow (l_1,R_1) \xrightarrow{(\alpha_1,p_1),\nu_1}\!\!\!\!\!\rightarrow \cdots \xrightarrow{(\alpha_{n-1},p_{n-1}),\nu_{n-1}}\!\!\!\!\!\rightarrow (l_n,R_n)$. Furthermore, for any "standard" region graph strategy π that is defined as a mapping from $FinRuns^{\mathcal{A}_k}$, a region graph strategy π' mapping from **PFinRuns** can be obtained by letting the choices of π' be the same as those of π for each potential finite run that has an associated finite run, and letting the choices of π' be arbitrary otherwise. Given that a potential finite run in **PFinRuns** that is without an associated finite run in $FinRuns^{\mathcal{A}_k}$ must correspond to probability 0, we have that $\mathbf{Pr}^{\mathrm{Pot},\pi'}_{(l,R)}(\Diamond^{\leq b}\mathbf{S}_F) = \mathbf{Pr}^{\pi}_{(l,R)}(\Diamond^{\leq b}\mathbf{S}_F)$. Vice versa, for any region graph strategy π mapping from **PFinRuns**, we can obtain "standard" region graph strategy mapping π' from $FinRuns^{\mathcal{A}_k}$ such that probabilities of $\Diamond^{\leq b}\mathbf{S}_F$ are the same for both strategies by letting π' make the same choice for a finite run as that made by π for the associated unique potential finite run. Hence considering region strategies that are mappings from **PFinRuns** does not change the maximum and minimum probabilities on the region graph $\mathcal{A}_k$.

We now describe formally how to obtain the cdPTA strategy $\sigma \in \mathbf{\Sigma}$, given $\pi \in \mathbf{\Pi}_k$ and $(l, R) \in L \times \mathsf{Regs}_k$. First we assume that $\pi \in \mathbf{\Pi}_k$ is *deterministic*, i.e., $|\mathsf{support}(\pi(r))| = 1$ for each $r \in \mathit{FinRuns}^{\mathcal{A}_k}$; in this case we write $\pi : \mathit{FinRuns}^{\mathcal{A}_k} \to \Gamma_k$ (rather than $\pi : \mathit{FinRuns}^{\mathcal{A}_k} \to \mathsf{Dist}(\Gamma_k)$). This assumption is without loss of generality, because, for a finite-state PTS such as $\mathcal{A}_k$, there exist deterministic strategies attaining the maximum and minimum values (see, for example, [21]). From π, we will construct a deterministic cdPTA strategy $\sigma \in \mathbf{\Sigma}$ and hence write $\sigma : \mathit{FinRuns}^{[\![\mathcal{P}]\!]} \to \Delta$ (rather than $\sigma : \mathit{FinRuns}^{[\![\mathcal{P}]\!]} \to \mathsf{Dist}(\Delta)$). Let $v \in R$ be an arbitrary valuation in R. We show how to construct σ inductively, starting from the state (l, v) and considering progressively longer runs (where the length of a run refers to its number of transitions).

Base case: run of length 0. Consider the choice of transition of π from (l, R). If $\pi(l, R) = ((l, R), \tau, \{(l, R') \mapsto 1\}) \in \overrightarrow{\Gamma_k}$, then we let $\sigma(l, v) = ((l, v), \delta, \{(l, v{+}\delta) \mapsto 1\})$ for some $\delta \in \mathbb{R}_{\geq 0}$ such that $v{+}\delta \in R'$ (the existence of transition $((l, v), \delta, \{(l, v + \delta) \mapsto 1\})$ follows from the fact that R' must be an $\mathit{inv}(l)$-satisfying time successor of R, by definition of $\overrightarrow{\Gamma_k}$).

If instead $\pi(l, R) = ((l, R), (\alpha, (l, g, \mathfrak{p})), \nu) \in \widehat{\Gamma_k}$, then we let $\sigma(l, v) = ((l, v), (l, g, \mathfrak{p}), \mu)$, i.e., we let $\sigma(l, v)$ be the (unique) transition from $\widehat{\Delta}$ generated from the probabilistic edge $(l, g, \mathfrak{p})$ (this transition must exist because $R \models g$ and $v \in R$ implies that $v \models g$).

Observe that, from Lemma 16, we can identify a bijection f_1 between the potential finite runs of length 1 of π and the finite runs of length 1 of σ. More precisely, for $((l, R) \xrightarrow{\tau, \{(l,R') \mapsto 1\}} (l, R')) \in \mathbf{PFinRuns}^{\pi}(l, R)$, we let $f_1((l, R) \xrightarrow{\tau, \{(l,R') \mapsto 1\}} (l', R')) = (l, v) \xrightarrow{\delta, \{(l, v+\delta) \mapsto 1\}} (l, v{+}\delta)$. Similarly, if instead $((l, R) \xrightarrow{(\alpha,(l,g,\mathfrak{p})),\nu} (l', R')) \in \mathbf{PFinRuns}^{\pi}(l, R)$, we let $f_1((l, R) \xrightarrow{(\alpha,(l,g,\mathfrak{p})),\nu} (l', R')) = (l, v) \xrightarrow{(l,g,\mathfrak{p}),\mu} (l', v')$ where $[\![l', v']\!]_k = (l', R')$.

Inductive step: runs of length n. Assume that we have defined σ for finite runs of length $n-1$, thereby obtaining a set of runs of length n. We now show how to define σ on these finite runs. Consider the finite run $r = (l_0, v_0) \xrightarrow{a_0,\mu_0} (l_1, v_1) \xrightarrow{a_1,\mu_1} \cdots \xrightarrow{a_{n-1},\mu_{n-1}} (l_n, v_n)$ of σ. As established by induction, there exists a bijection f_n between the potential finite runs of length n of π and the finite runs of length n of σ. Consider the potential finite run $f_n^{-1}(r)$ of π, and write (l_n, R_n) for $\mathit{last}(f_n^{-1}(r))$. The construction proceeds in a similar manner to that for the base case. If $\pi(f_n^{-1}(r)) \in \overrightarrow{\Gamma_k}$ where $\pi(f_n(r)) = ((l_n, R_n), \tau, \{(l_n, R') \mapsto 1\})$, then we let $\sigma(r) = ((l_n, v_n), \delta, \{(l_n, v_n{+}\delta) \mapsto 1\})$ for some $\delta \in \mathbb{R}_{\geq 0}$ such that $v_n{+}\delta \in R'$. Furthermore, $f_{n+1}(f_n^{-1}(r) \xrightarrow{\tau, \{(l_n,R') \mapsto 1\}} (l_n, R')) = r \xrightarrow{\delta, \{(l, v_n+\delta) \mapsto 1\}} (l_n, v_n{+}\delta)$.

If instead $\pi(f_n^{-1}(r)) \in \widehat{\Gamma_k}$, where $\pi(f_n^{-1}(r)) = ((l_n, R_n), (\alpha, (l_n, g, \mathfrak{p})), \nu)$, then we let $\sigma(r) = ((l_n, v_n), (l_n, g, \mathfrak{p}), \mu)$, i.e., $\sigma(l, v)$ is the transition from $\widehat{\Delta}$ generated from the probabilistic edge $(l_n, g, \mathfrak{p})$. Then for $f_n^{-1}(r) \xrightarrow{(\alpha,(l_n,g,\mathfrak{p})),\nu} (l', R') \in \mathbf{PFinRuns}^{\pi}(l, R)$, we let $f_{n+1}(f_n^{-1}(r) \xrightarrow{(\alpha,(l_n,g,\mathfrak{p})),\nu} (l', R')) = r \xrightarrow{(l_n,g,\mathfrak{p}),\mu} (l', v')$ where $[\![l', v']\!]_k = (l', R')$.

Repeating this approach for all runs of length n then yields a definition of σ and of f_{n+1}.

Given the state $(l, v) \in S$ and the deterministic region graph strategy $\pi \in \mathbf{\Pi}_k$, the *mimicking strategy for* (l, v) *and* π is the deterministic cdPTA strategy $\sigma \in \mathbf{\Sigma}$ obtained by the above construction.

Consider the MCs $\mathcal{M}^{\sigma}_{(l,v)} = (\mathit{FinRuns}^{\sigma}(l, v), (l, v), \mathbf{P}^{\sigma}_{(l,v)})$ and $\mathcal{M}^{\mathrm{Pot},\pi}_{(l,R)} = (\mathbf{PFinRuns}^{\pi}(l, R), (l, R), \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)})$. Let $f : \mathbf{PFinRuns}^{\pi}(l, R) \to \mathit{FinRuns}^{\sigma}(l, v)$ be such

that, for a potential finite run $\rho \in \mathbf{PFinRuns}^{\pi}(l,R)$ of length n, we have $f(\rho) = f_n(\rho)$. We now show that the equivalence relation induced by f on the disjoint union of $\mathcal{M}^{\sigma}_{(l,v)}$ and $\mathcal{M}^{\mathrm{Pot},\pi}_{(l,R)}$ is an ϵ-bisimulation, where ϵ depends on the cdPTA and on the granularity k. Formally, we define the equivalence relation $\mathcal{R}_f \subseteq \mathit{FinRuns}^{\sigma}(l,v) \times \mathbf{PFinRuns}^{\pi}(l,R)$ as the smallest set such that, for $r \in \mathit{FinRuns}^{\sigma}(l,v)$ and $\rho \in \mathbf{PFinRuns}^{\pi}(l,R)$, if $f(\rho) = r$ then $(r,\rho) \in \mathcal{R}_f$. In order to show that the equivalence relation $\mathcal{R}_f$ is an ϵ-bisimulation, we show that the distributions chosen from equivalent finite paths generated by σ and π are sufficiently "close". Consider $r \in \mathit{FinRuns}^{\sigma}(l,v)$ and $\rho \in \mathbf{PFinRuns}^{\pi}(l,R)$ such that $(r,\rho) \in \mathcal{R}_f$. In the following, we use $(\tilde{l},\tilde{v})$ to denote $\mathit{last}(r)$ and $(\tilde{l},\tilde{R})$ to denote $\mathit{last}(\rho)$ (note that $(r,\rho) \in \mathcal{R}_f$ guarantees that $\mathit{last}(r)$ and $\mathit{last}(\rho)$ have the same location component $\tilde{l}$). We focus primarily on the case in which $\sigma(r) \in \widehat{\Delta}$ and $\pi(\rho) \in \widehat{\Gamma_k}$: we let $\sigma(r) = ((\tilde{l},\tilde{v}),p,\mu)$ and $\pi(\rho) = ((l,\tilde{R}),(\alpha,p),\nu)$. Note that, by the construction of σ, the same probabilistic edge $p = (\tilde{l},g,\mathfrak{p})$ is used for both $\sigma(r)$ and $\pi(\rho)$. Given an outcome $e \in 2^{\mathcal{X}} \times L$, let $\breve{d}^{p,e} = \max_{x\in\mathcal{X}} |d^{p,e}_x|$.

Lemma 17. *Let $\alpha \in \mathsf{CP}(\tilde{R})$ and let $e \in 2^{\mathcal{X}} \times L$. Then $|\mathfrak{p}[\tilde{v}](e) - \mathfrak{p}[\alpha](e)| < \frac{|\mathcal{X}|\cdot\breve{d}^{p,e}}{k}$.*

Proof. Note that, by the definition of $\mathsf{CP}(\tilde{R})$, we have $|(\tilde{v}(x) - \alpha(x))| < \frac{1}{k}$ for each $x \in \mathcal{X}$. By definition, for $\beta \in \{\tilde{v},\alpha\}$, we have $\mathfrak{p}[\beta](e) = \sum_{x\in\mathcal{X}} f^{p,e}_x(\beta(x)) = \sum_{x\in\mathcal{X}}(c^{p,e}_x + d^{p,e}_x \cdot \beta(x)) = \sum_{x\in\mathcal{X}} c^{p,e}_x + \sum_{x\in\mathcal{X}} d^{p,e}_x \cdot \beta(x)$. Hence:

$$\begin{aligned} |\mathfrak{p}[\tilde{v}](e) - \mathfrak{p}[\alpha](e)| &= |\sum_{x\in\mathcal{X}} d^{p,e}_x \cdot \tilde{v}(x) - \sum_{x\in\mathcal{X}} d^{p,e}_x \cdot \alpha(x)| \\ &\leq \sum_{x\in\mathcal{X}} d^{p,e}_x |(\tilde{v}(x) - \alpha(x))| < \sum_{x\in\mathcal{X}} d^{p,e}_x \cdot \frac{1}{k} \leq \frac{|\mathcal{X}|\cdot\breve{d}^{p,e}}{k} . \end{aligned}$$

□

We now generalise Lemma 17 from outcomes to target states. Let $\breve{d}^{p} = \max_{e\in 2^{\mathcal{X}}\times L} \breve{d}^{p,e}$ and, for $l' \in L$, let $\mathit{OutLoc}[\tilde{R}](p,l') = |\{(X,l'') \in \mathsf{support}[\tilde{R}](p) : l'' = l'\}|$ be the number of outcomes leading to location l' that are assigned positive probability for p from valuations within $\tilde{R}$.

Lemma 18. *Let $((\tilde{l},\tilde{v}),p,\mu) \in \widehat{\Delta}$, let $((l,\tilde{R}),(\alpha,p),\nu) \in \widehat{\Gamma_k}$, and let $(l',v') \in \mathsf{support}(\mu)$. Then $|\mu(l',v') - \nu(\langle\!|l',v'|\!\rangle_k)| < \frac{\mathit{OutLoc}[\tilde{R}](p,l')\cdot|\mathcal{X}|\cdot\breve{d}^{p}}{k}$.*

Proof. Let $p = (\tilde{l},g,\mathfrak{p})$. Using $(l',R') \in L \times \mathsf{Regs}_k$ to denote $\langle\!|l',v'|\!\rangle_k$, we recall that, by definition, $\mu(l',v') = \sum_{X\in\mathsf{Reset}(\tilde{v},v')} \mathfrak{p}[\tilde{v}](X,l')$ and $\nu(l',R') = \sum_{X\in\mathsf{Reset}(\tilde{R},R')} \mathfrak{p}[\alpha](X,l')$. By Lemma 1, we have $\mathsf{Reset}(\tilde{v},v') = \mathsf{Reset}(\tilde{R},R')$, and hence:

$$\begin{aligned} |\mu(l',v') - \nu(\langle\!|l',v'|\!\rangle_k)| &= \Big|\sum_{X\in\mathsf{Reset}(\tilde{v},v')} \mathfrak{p}[\tilde{v}](X,l') - \sum_{X\in\mathsf{Reset}(\tilde{R},R')} \mathfrak{p}[\alpha](X,l')\Big| \\ &= \Big|\sum_{X\in\mathsf{Reset}(\tilde{v},v')} \mathfrak{p}[\tilde{v}](X,l') - \sum_{X\in\mathsf{Reset}(\tilde{v},v')} \mathfrak{p}[\alpha](X,l')\Big| \\ &\leq \sum_{X\in\mathsf{Reset}(\tilde{v},v')} |\mathfrak{p}[\tilde{v}](X,l') - \mathfrak{p}[\alpha](X,l')| . \end{aligned}$$

Furthermore, from Lemma 17, for all $e \in 2^{\mathcal{X}} \times L$, we have $|\mathfrak{p}[\tilde{v}](e) - \mathfrak{p}[\alpha](e)| < \frac{|\mathcal{X}|\cdot\breve{d}^{p,e}}{k} \leq \frac{|\mathcal{X}|\cdot\breve{d}^{p}}{k}$. Note that, from the definition of $\mathsf{support}[\tilde{R}](p)$, for any $(X,l') \notin \mathsf{support}[\tilde{R}](p)$, we have

$\mathfrak{p}[v'](X,l') = 0$ for all $v' \in \tilde{R}$ (and hence $\mathfrak{p}[\tilde{v}](X,l') = 0$). Furthermore, this fact implies that, for $(X,l') \notin \mathsf{support}[\tilde{R}](p)$, we have $\mathfrak{p}[\alpha](X,l') = 0$ for all $\alpha \in \mathsf{CP}(R)$, given that (1) $\mathfrak{p}[\cdot](X,l')$ is a constant function over valuations in $\tilde{R}$, (2) $\mathfrak{p}[\cdot](X,l')$ is a continuous function over valuations in the closure of $\tilde{R}$, and (3) α corresponds to a point in the closure of $\tilde{R}$. Overall, this means that $(X,l') \notin \mathsf{support}[\tilde{R}](p)$ implies that $|\mathfrak{p}[\tilde{v}](X,l') - \mathfrak{p}[\alpha](X,l')| = 0$. In turn, this means that:

$$\begin{aligned}
\sum_{X \in \mathsf{Reset}(\tilde{v},v')} |\mathfrak{p}[\tilde{v}](X,l') - \mathfrak{p}[\alpha](X,l')| &= \sum_{X \in \mathsf{Reset}(\tilde{v},v') \wedge (X,l') \in \mathsf{support}[\tilde{R}](p)} |\mathfrak{p}[\tilde{v}](X,l') - \mathfrak{p}[\alpha](X,l')| \\
&\leq \sum_{X \subseteq \mathcal{X} \wedge (X,l') \in \mathsf{support}[\tilde{R}](p)} |\mathfrak{p}[\tilde{v}](X,l') - \mathfrak{p}[\alpha](X,l')| \\
&< \frac{\mathit{OutLoc}[\tilde{R}](p,l') \cdot |\mathcal{X}| \cdot \breve{d}^p}{k} .
\end{aligned}$$

□

Let $\breve{d} = \max_{p \in \mathit{prob}} \breve{d}^p$ be the maximum absolute value of the gradient of any clock in any clock dependency of the cdPTA, let $\mathit{MaxOutLoc} = \max_{(R',p,l') \in \mathsf{Regs}_k \times \mathit{prob} \times L} \mathit{OutLoc}[R'](p,l')$ be the maximum number of outcomes of any probabilistic edge leading to the same location, and let $\mathit{MaxOut} = \max_{(R',p) \in \mathsf{Regs}_k \times \mathit{prob}} \mathsf{support}[R'](p)$ be the maximum number of outcomes that can be associated positive probability by any probabilistic edge. The main result of this section now follows.

Proposition 5. *Let $k \in \mathbb{N}$, let $(l,v) \in S$ and let $\pi \in \mathbf{\Pi}_k$ be a deterministic region graph strategy. Then there exists a deterministic cdPTA strategy $\sigma \in \mathbf{\Sigma}$ such that $\mathcal{R}_f$ is an ϵ-bisimulation on the disjoint union of $\mathcal{M}^{\sigma}_{(l,v)}$ and $\mathcal{M}^{\mathrm{Pot},\pi}_{\langle\!\langle l,v \rangle\!\rangle_k}$, where $\epsilon = \frac{\mathit{MaxOutLoc} \cdot |\mathcal{X}| \cdot \breve{d} \cdot \mathit{MaxOut}}{k}$.*

Proof. Let $\sigma \in \mathbf{\Sigma}$ be the mimicking strategy for (l,v) and π. In the following, we use (l,R) to denote $\langle\!\langle l,v \rangle\!\rangle_k$. Consider the MCs $\mathcal{M}^{\sigma}_{(l,v)} = (\mathit{FinRuns}^{\sigma}(l,v), (l,v), \mathbf{P}^{\sigma}_{(l,v)})$ and $\mathcal{M}^{\mathrm{Pot},\pi}_{(l,R)} = (\mathbf{PFinRuns}^{\pi}(l,R), (l,R), \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)})$. Let $r \in \mathit{FinRuns}^{\sigma}(l,v)$ and $\rho \in \mathbf{PFinRuns}^{\pi}(l,R)$ be such that $(r,\rho) \in \mathcal{R}_f$. As above, we use $(\tilde{l},\tilde{v})$ to denote $\mathit{last}(r)$ and $(\tilde{l},\tilde{R})$ to denote $\mathit{last}(\rho)$. We first show that, for $r' \in \mathit{FinRuns}^{\sigma}(l,v)$ and $\rho' \in \mathbf{PFinRuns}^{\pi}(l,R)$ for which $(r',\rho') \in \mathcal{R}_f$ and for which the length of r' and ρ' is equal to the length of r and ρ plus 1, we have $|\mathbf{P}^{\sigma}_{(l,v)}(r,r') - \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho')| < \frac{\mathit{MaxOutLoc} \cdot |\mathcal{X}| \cdot \breve{d}}{k}$. We have two cases:

Case $\pi(\rho) \in \overrightarrow{\Gamma_k}$**:** If $\pi(\rho) = ((\tilde{l},\tilde{R}), \tau, \{(\tilde{l},R') \mapsto 1\}) \in \overrightarrow{\Gamma_k}$, then the construction of σ specifies that $\sigma(r) = ((\tilde{l},\tilde{v}), \delta, \{(l, \tilde{v}{+}\delta) \mapsto 1\})$ for some $\delta \in \mathbb{R}_{\geq 0}$ such that $\tilde{v}{+}\delta \in R'$. Then $r' = r \xrightarrow{\delta,\{(l,v_n+\delta) \mapsto 1\}} (l_n, v_n{+}\delta)$ and $\rho' = \rho \xrightarrow{\tau,\{(\tilde{l},R') \mapsto 1\}} (\tilde{l},R')$. Given that, by the construction of σ, we have $f_{n+1}(\rho') = r'$, it follows that $(r',\rho') \in \mathcal{R}_f$. Furthermore, we note that $\mathbf{P}^{\sigma}_{(l,v)}(r,r') = \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho') = 1$, and hence trivially $|\mathbf{P}^{\sigma}_{(l,v)}(r,r') - \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho')| = 0 < \frac{\mathit{MaxOutLoc} \cdot |\mathcal{X}| \cdot \breve{d}}{k}$.

Case $\pi(\rho) \in \widehat{\Gamma_k}$**:** If $\pi(\rho) = ((\tilde{l},\tilde{R}), (\alpha, (\tilde{l},g,\mathfrak{p})), \nu) \in \widehat{\Gamma_k}$, then the construction of σ specifies that $\sigma(r) = ((\tilde{l},\tilde{v}), (\tilde{l},g,\mathfrak{p}), \mu)$. Let $\mathsf{support}(\mu) = \{(l_1,v_1), \ldots, (l_m,v_m)\}$. Then $\mathsf{PT}(\langle\!\langle l,v \rangle\!\rangle_k, (l,g,\mathfrak{p})) = \{\langle\!\langle l_1,v_1 \rangle\!\rangle_k, \ldots, \langle\!\langle l_m,v_m \rangle\!\rangle_k\}$ where $\langle\!\langle l_i,v_i \rangle\!\rangle_k \neq \langle\!\langle l_j,v_j \rangle\!\rangle_k$ for all $i,j \in \{1,\ldots,m\}$ such that $i \neq j$, by Lemma 16. Consider i such that $i \in \{1,\ldots,m\}$, and let $r_i = r \xrightarrow{(\tilde{l},g,\mathfrak{p}),\mu} (l_i,v_i)$ and $\rho_i = \rho \xrightarrow{(\alpha,(\tilde{l},g,\mathfrak{p})),\nu} \langle\!\langle l_i,v_i \rangle\!\rangle_k$. Furthermore, we have defined $f : \mathbf{PFinRuns}^{\pi}(l,R) \to \mathit{FinRuns}^{\sigma}(l,v)$ such that $f(\rho_i) = r_i$ for each $i \in \{1,\ldots,m\}$, and hence $(r_i,\rho_i) \in \mathcal{R}_f$. Then the fact that $|\mathbf{P}^{\sigma}_{(l,v)}(r,r_i) - \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho_i)| < \frac{\mathit{MaxOutLoc} \cdot |\mathcal{X}| \cdot \breve{d}}{k}$ follows directly from Lemma 18 and the definitions of $\mathit{MaxOutLoc}$ and $\breve{d}$.

Now consider $r \in \mathit{FinRuns}^\sigma(l,v)$ and $\rho \in \mathbf{PFinRuns}^\pi(l,R)$ such that $(r,\rho) \in \mathcal{R}_f$. In order to show that $\mathcal{R}_f$ is an ϵ-bisimulation, we require that (1) $\mathit{last}(r) \in S_F$ if and only if $\mathit{last}(\rho) \in \mathsf{Regs}^F_k$, (2a) $\mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho, \mathcal{R}_f(E)) \geq \mathbf{P}^\sigma_{(l,v)}(r,E) - \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}\cdot\mathit{MaxOut}}{k}$ for $E \subseteq \mathit{FinRuns}^\sigma(l,v)$, and (2b) $\mathbf{P}^\sigma_{(l,v)}(r, \mathcal{R}_f(\mathbf{E})) \geq \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\mathbf{E}) - \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}\cdot\mathit{MaxOut}}{k}$ for $\mathbf{E} \subseteq \mathbf{PFinRuns}^\pi(l,R)$. Requirement (1) follows directly from the fact that the location components of the states $\mathit{last}(r)$ and $\mathit{last}(\rho)$ are identical. Now we show that requirement (2a) holds. First note that $\mathcal{R}_f(E) = \{f(r) : r \in E\}$. Also note that $\mathbf{P}^\sigma_{(l,v)}(r,E) = \sum_{r' \in E} \mathbf{P}^\sigma_{(l,v)}(r,r')$, and similarly $\mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho, \mathcal{R}_f(E)) = \sum_{\rho' \in \mathcal{R}_f(E)} \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho') = \sum_{r' \in E} \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho, f(r'))$. We can assume that E only contains finite runs that are successor runs of r under σ, because $\mathbf{P}^\sigma_{(l,v)}(r,r') = 0$ for all finite other runs r'. Under this assumption, $|E| \leq \mathit{MaxOut}$. Furthermore, we can observe that $\mathcal{R}_f(E)$ will contain only potential finite runs that are obtained from ρ under π. We have established above that $|\mathbf{P}^\sigma_{(l,v)}(r,r') - \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho')| < \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}}{k}$ for $(r,\rho),(r',\rho') \in \mathcal{R}_f$ (where r' and ρ' are obtained by extending r and ρ, respectively, with one transition). Hence, for $r' \in E$, we have $\mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho, f(r')) \geq \mathbf{P}^\sigma_{(l,v)}(r,r') - \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}}{k}$. Then $\mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho, \mathcal{R}_f(E)) = \sum_{\rho' \in \mathcal{R}_f(E)} \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\rho') = \sum_{r' \in E} \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho, f(r')) \geq \sum_{r' \in E}(\mathbf{P}^\sigma_{(l,v)}(r,r') - \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}}{k}) \geq \mathbf{P}^\sigma_{(l,v)}(r,E) - \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}\cdot\mathit{MaxOut}}{k}$.

It remains to show requirement (2b), i.e., $\mathbf{P}^\sigma_{(l,v)}(r, \mathcal{R}_f(\mathbf{E})) \geq \mathbf{P}^{\mathrm{Pot},\pi}_{(l,R)}(\rho,\mathbf{E}) - \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}\cdot\mathit{MaxOut}}{k}$ for $\mathbf{E} \subseteq \mathbf{PFinRuns}^\pi(l,R)$. We can proceed in a similar manner to case (2a), and omit the details. □

The combination of Proposition 4 and Proposition 5 give us the following corollary, where we assume that k, (l,v), π and ϵ are as in the statement of Proposition 5, that $b \in \mathbb{N}$, and that $\mathbf{S}_F$ is the set of states of the disjoint union of the MCs $\mathcal{M}^\sigma_{(l,v)}$ and $\mathcal{M}^{\mathrm{Pot},\pi}_{(l,R)}$ that end in a state with location component in $F \subseteq L$.

Corollary 3. *The mimicking strategy σ for (l,R) and π is such that*

$$|\mathbf{Pr}^\sigma_{(l,v)}(\Diamond^{\leq b}\mathbf{S}_F) - \mathbf{Pr}^\pi_{(\!|l,v|\!)_k}(\Diamond^{\leq b}\mathbf{S}_F)| \leq 1 - (1-\epsilon)^b \,.$$

Proposition 3 leads to the following approach for maximal and minimal reachability problems for b-step-bounded cdPTA. Let $\epsilon_k = \frac{\mathit{MaxOutLoc}\cdot|\mathcal{X}|\cdot\breve{d}\cdot\mathit{MaxOut}}{k}$. Consider the case for the maximal reachability problem, which we recall involves deciding whether $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!],\mathbf{\Sigma}}(S_F) \trianglerighteq \lambda$. After selecting an initial $k \in \mathbb{N}$, construct $\mathcal{A}_k$ and compute $\mathbb{P}^{\max}_{\mathcal{A}_k,\mathbf{\Pi}_k}(S_F)$. If $\mathbb{P}^{\max}_{\mathcal{A}_k,\mathbf{\Pi}_k}(S_F) - (1-(1-\epsilon_k)^b) \trianglerighteq \lambda$, we conclude that $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!],\mathbf{\Sigma}}(S_F) \trianglerighteq \lambda$ holds. If, instead, $\mathbb{P}^{\max}_{\mathcal{A}_k,\mathbf{\Pi}_k}(S_F) \not\trianglerighteq \lambda$ then, by Proposition 2, we conclude that $\mathbb{P}^{\max}_{[\![\mathcal{P}]\!],\mathbf{\Sigma}}(S_F) \not\trianglerighteq \lambda$. The remaining possibility (that is, when $\mathbb{P}^{\max}_{\mathcal{A}_k,\mathbf{\Pi}_k}(S_F) - (1-(1-\epsilon_k)^b) \not\trianglerighteq \lambda$ and $\mathbb{P}^{\max}_{\mathcal{A}_k,\mathbf{\Pi}_k}(S_F) \trianglerighteq \lambda$) is inconclusive; hence, as in Section 4.2, we choose some $n \geq 1$, and repeat the above process using $2^n \cdot k$ instead of k. Note that this approach can establish both positive and negative answers to the maximal reachability problem, unlike the approach of Section 4.2, which can only establish negative answers. A similar approach can be taken for minimum reachability problems.

4.4 Application to Examples 1 and 2

We now consider the application of the results of this section to Examples 1 and 2.

Example 6. *We give the intuition underlying Proposition 2 and Proposition 3 using the cdPTA of Example 2 (Figure 2), considering the maximum probability of reaching the target location* D. *When $k = 1$, as described above, the maximum probability of reaching* D *is*

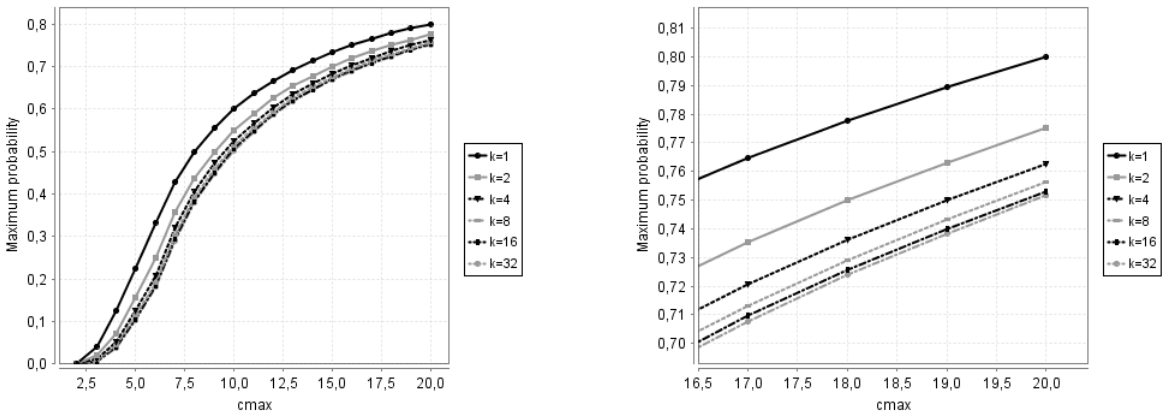

Figure 9: Maximum probability of reaching location ✓ in the cdPTA of Figure 1. (Left) Results for $k \in \{2^0, 2^1, ..., 2^5\}$ and $c_{\max} \in \{2, ..., 20\}$. (Right) Magnified view of the results for $k \in \{2^0, 2^1, ..., 2^5\}$ and $c_{\max} \in \{17, 18, 19, 20\}$.

1. *Instead, for* $k = 2$*, the maximum probability of reaching location* D *requires taking the probabilistic edge from location* A *for the corner point* $x = \frac{1}{2}$ *corresponding to the* 2*-region* $0 < x < \frac{1}{2}$ *and the probabilistic edges from locations* B *and* C *for corner point* $x = 0$*, again for the* 2*-region* $0 < x < \frac{1}{2}$ *i.e., the probability is* $\frac{1}{2}$*. With granularity* $k = 4$*, the maximum probability of reaching location* D *is* 0.328125*, obtained by taking the probabilistic edge from* A *for the corner point* $x = \frac{1}{2}$*, and the probabilistic edges from* B *and* C *for corner point* $x = \frac{1}{4}$*, where the* 4*-region used in all cases is* $\frac{1}{4} < x < \frac{1}{2}$*.*

Example 7. *In Figure 9 we plot the values of the maximum probability of reaching location* ✓ *in the cdPTA of Example 1 (Figure 1) for various values of* $c_{\max}$ *and* k*, obtained by encoding the clock-dependent region graph as a finite-state PTS and using* Prism *[22]. For this example, the difference between the probabilities obtained for various values of* k *decreases substantially as greater values of* k *are considered, as emphasised by focussing on a limited number of values of* $c_{\max}$ *on the right of Figure 9. For* $c_{\max} = 20$*, the number of states of the clock-dependent region graphs ranges from* 3444 *for* $k = 1$*,* 12866 *for* $k = 2$*,* 49638 *for* $k = 4$*,* 194894 *for* $k = 8$*,* 772254 *for* $k = 16$*, to* 3074366 *for* $k = 32$*. Note that both this and the previous examples are* b*-step-bounded cdPTA: for Example 2 we have* $b = 6$*, and for Example 1 we have* $b = 2(c_{\max} + 1)$*.*

5 Conclusion

In this paper we presented cdPTA, an extension of PTA in which probabilities can depend on the values of clocks. We have shown that a basic probabilistic model checking problem, maximal reachability, is undecidable for cdPTA with at least three clocks. We also presented a conservative overapproximation method for cdPTA, and presented bounds on the degree of approximation for a subclass of cdPTA. One direction of future research could concern identifying other kinds of subclass of cdPTA for which for which probabilistic reachability problems are decidable. Furthermore, we conjecture that qualitative reachability problems (whether there exists a strategy such that the target locations are reached with probability strictly greater than 0, or equal to 1) are decidable (and in exponential time) for cdPTA for which the linear functions are bounded away from 0, by a region graph construction. The case of linear functions that can approach arbitrarily closely to 0 requires more care: although concepts introduced for qualitative reachability problems for open interval Markov

chains [23] can be used as a starting point, the issue of non-forgetful cycles, in the terminology of [24], present a challenge, because they can prevent the convergence of a probability of a cdPTA run to 0. Finally, the issue of the expressiveness of cdPTA in relation to other modelling formalisms, such as stochastic timed automata [25] or stochastic timed Markov decision processes [9], could be explored.

Acknowledgments

The inspiration for cdPTA arose from a discussion with Patricia Bouyer on the corner-point abstraction. Thanks also to Holger Hermanns, who expressed interest in a cdPTA-like formalism in a talk at Dagstuhl Seminar 14441, and to Devendra Bhave, who suggested a simplification to the cdPTA formalism as presented at RP 2017.

References

[1] Gregersen H, Jensen HE. Formal Design of Reliable Real Time Systems. Master's thesis, Department of Mathematics and Computer Science, Aalborg University, 1995.

[2] Kwiatkowska M, Norman G, Segala R, Sproston J. Automatic verification of real-time systems with discrete probability distributions. *Theoretical Computer Science*, 2002. **286**:101–150. doi:10.1016/S0304-3975(01)00046-9.

[3] Alur R, Dill DL. A theory of timed automata. *Theoretical Computer Science*, 1994. **126**(2):183–235. doi:10.1016/0304-3975(94)90010-8.

[4] Puterman ML. Markov Decision Processes. J. Wiley & Sons, 1994.

[5] Segala R. Modeling and Verification of Randomized Distributed Real-Time Systems. Ph.D. thesis, Massachusetts Institute of Technology, 1995.

[6] Kwiatkowska M, Norman G, Parker D, Sproston J. Performance Analysis of Probabilistic Timed Automata using Digital Clocks. *Formal Methods in System Design*, 2006. **29**:33–78. doi:10.1007/s10703-006-0005-2.

[7] Norman G, Parker D, Sproston J. Model Checking for Probabilistic Timed Automata. *Formal Methods in System Design*, 2013. **43**(2):164–190. doi:10.1007/s10703-012-0177-x.

[8] Abate A, Katoen J, Lygeros J, Prandini M. Approximate Model Checking of Stochastic Hybrid Systems. *European Journal of Control*, 2010. **16**(6):624–641. doi:10.3166/ejc.16.624-641.

[9] Akshay S, Bouyer P, Krishna SN, Manasa L, Trivedi A. Stochastic Timed Games Revisited. In: Proc. 41st International Symposium on Mathematical Foundations of Computer Science (MFCS'16), volume 58 of *LIPIcs*. Leibniz-Zentrum für Informatik, 2016 pp. 8:1–8:14. doi:10.4230/LIPIcs.MFCS.2016.8.

[10] Bouyer P, Brinksma E, Larsen KG. Optimal Infinite Scheduling for Multi-Priced Timed Automata. *Formal Methods in System Design*, 2008. **32**(1):2–23. doi:10.1007/s10703-007-0043-4.

[11] Sproston J. Probabilistic Timed Automata with Clock-Dependent Probabilities. In: Hague M, Potapov I (eds.), Proc. RP 2017, volume 10506 of *LNCS*. Springer, 2017 pp. 144–159. doi:10.1007/978-3-319-67089-8_11.

[12] Sproston J. Probabilistic Timed Automata with Clock-Dependent Probabilities. *Fundamenta Informaticae*, 2021. **178**(1–2):101–138. doi:10.3233/FI-2021-2000.

[13] Hahn EM. Model checking stochastic hybrid systems. Ph.D. thesis, Universität des Saarlandes, 2013.

[14] Kemeny JG, Snell JL, Knapp AW. Denumerable Markov Chains. Graduate Texts in Mathematics. Springer, 2nd edition, 1976.

[15] Jurdziński M, Laroussinie F, Sproston J. Model Checking Probabilistic Timed Automata with One or Two Clocks. *Logical Methods in Computer Science*, 2008. **4**(3):1–28. doi:10.2168/LMCS-4(3:12)2008.

[16] Minsky M. Computation: Finite and Infinite Machines. Prentice Hall International, 1967.

[17] Bouyer P. On the optimal reachability problem in weighted timed automata and games. In: Proc. 7th Workshop on Non-Classical Models of Automata and Applications (NCMA'15), volume 318 of *books@ocg.at*. Austrian Computer Society, 2015 pp. 11–36.

[18] Desharnais J, Laviolette F, Tracol M. Approximate Analysis of Probabilistic Processes: Logic, Simulation and Games. In: Proc. 5th International Conference on the Quantitative Evaluaiton of Systems (QEST'08). IEEE Computer Society, 2008 pp. 264–273. doi:10.1109/QEST.2008.42.

[19] Bian G, Abate A. On the Relationship Between Bisimulation and Trace Equivalence in an Approximate Probabilistic Context. In: Proc. of the 20th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'17), volume 10203 of *LNCS*. 2017 pp. 321–337. doi:10.1007/978-3-662-54458-7_19.

[20] Tripakis S, Yovine S, Bouajjani A. Checking Timed Büchi Automata Emptiness Efficiently. *Formal Methods in System Design*, 2005. **26**(3):267–292. doi:10.1007/s10703-005-1632-8.

[21] Baier C, Katoen J. Principles of model checking. MIT Press, 2008.

[22] Kwiatkowska M, Norman G, Parker D. PRISM 4.0: Verification of Probabilistic Real-time Systems. In: Proc. 23rd International Conference on Computer Aided Verification (CAV'11), volume 6806 of *LNCS*. Springer, 2011 pp. 585–591. doi:10.1007/978-3-642-22110-1_47.

[23] Sproston J. Qualitative Reachability for Open Interval Markov Chains. In: Potapov I, Reynier PA (eds.), Proc. RP 2018, volume 11123 of *LNCS*. Springer, 2018 pp. 146–160. doi:10.1007/978-3-030-00250-3_11.

[24] Basset N, Asarin E. Thin and Thick Timed Regular Languages. In: Proc. of the 9th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'11), volume 6919 of *LNCS*. Springer, 2011 pp. 113–128. doi:10.1007/978-3-642-24310-3_9.

[25] Bohnenkamp HC, D'Argenio PR, Hermanns H, Katoen J. MODEST: A Compositional Modeling Formalism for Hard and SoftlyTimed Systems. *IEEE Transactions on Software Engineering*, 2006. **32**(10):812–830. doi:10.1109/TSE.2006.104.